

Directory and Resource Administrator 10.2.3 Administrator Guide

November 2023

Legal Notice

For information about legal notices, trademarks, disclaimers, warranties, export and other use restrictions, U.S. Government rights, patent policy, and FIPS compliance, see <https://www.microfocus.com/en-us/legal>.

© Copyright 2007 – 2023 Open Text or one of its affiliates.

The only warranties for products and services of Open Text and its affiliates and licensors (“Open Text”) are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Open Text shall not be liable for technical or editorial errors or omissions contained herein. The information contained herein is subject to change without notice.

Contents

About this Guide	11
Part I Getting Started	13
1 What is Directory and Resource Administrator	15
2 Understanding Directory and Administrator Components	17
DRA Administration Server	17
Delegation and Configuration Console	18
Web Console	18
Reporting Components	18
Workflow Automation Engine	19
Product Architecture	20
Part II Product Installation and Upgrade	21
3 Planning Your Deployment	23
Tested Resource Recommendations	23
Virtual Environment Resource Provisioning	23
Required Ports and Protocols	24
DRA Administration Servers	24
DRA REST Server	26
Web Console (IIS)	26
DRA Delegation and Administration Console	26
Workflow Server	27
Supported Platforms	27
DRA Administration Server and Web Console Requirements	29
Software Requirements	29
Server Domain	31
Account Requirements	31
Least Privilege DRA Access Accounts	33
Reporting Requirements	37
Software Requirements	37
Licensing Requirements	38
Language Support	38
1. Web Browser Language Localization:	38
2. Localized Character Support for Object Names:	38
3. DRA Installation in Non-English Localized Operating System:	39
4. Windows Domain Controllers with Full Localization:	39
4 Product Installation	41
Install the DRA Administration Server	41

Interactive Installation Checklist:	42
Install DRA Clients	43
Install Workflow Automation and Configure Settings	44
Install DRA Reporting	44
5 Product Upgrade	47
Planning a DRA Upgrade	47
Pre-Upgrade Tasks	48
Dedicating a Local Administration Server to Run a Previous DRA Version	49
Synchronizing Your Previous DRA Version Server Set	50
Backing Up the Administration Server Registry	50
Upgrading the DRA Administration Server	51
Upgrading the Primary Administration Server	52
Installing a Local Secondary Administration Server for the Current DRA Version	52
Deploying the DRA User Interfaces	53
Upgrading Secondary Administration Servers	53
Updating the Web Console Configuration - Post Installation	54
Upgrading Workflow Automation	54
Upgrading Reporting	55
Part III Delegation Model	57
6 Understanding the Dynamic Delegation Model	59
Delegation Model Controls	59
How DRA Processes Requests	60
Examples of How DRA Processes Delegation Assignments	60
Example 1: Changing a User's Password	60
Example 2: Overlapping ActiveViews	60
7 ActiveViews	65
Built-in ActiveViews	65
Accessing Built-in ActiveViews	66
Using Built-in ActiveViews	66
Implementing a Custom ActiveView	66
ActiveViews Rules	68
8 Roles	69
Built-in Roles	69
Azure Active Directory Management	69
Administration	70
Advanced Query Management	71
Audit Management	71
Computer Management	71
Exchange Management	72
Group Management	73
Reporting Management	74
Resource Management	74
Server Management	75
User Account Management	76

WTS Administration	77
Accessing Built-in Roles	77
Using Built-in Roles	78
Creating Custom Roles	78
9 Powers	79
Built-in Powers	79
Azure Powers	79
Implementing Custom Powers	80
Extending Powers	81
10 Delegation Assignments	83
Part IV Component and Process Configuration	85
11 Initial Configuration	87
Configuration Checklist	87
Installing or Upgrading Licenses	88
Configure DRA Servers and Features	88
Configuring the Multi-Master Set	89
Managing Clone Exceptions	91
File Replication	91
Azure Sync	94
Enabling Multiple Managers for Groups	94
Encrypted Communications	95
Defining Virtual Attributes	95
Configuring Caching	96
Enabling Active Directory Printers Collection	99
AD LDS	99
Dynamic Group	99
Configuring the Recycle Bin	99
Reporting Configuration	100
Delegating Workflow Automation Server Configuration Powers	102
Configuring the Workflow Automation Server	103
Delegating the LDAP Search Powers	103
Configuring Change History Reporting	104
Install the Change Guardian Windows Agent	105
Add an Active Directory License key	105
Configure Active Directory	105
Create and Assign an Active Directory Policy	108
Manage Active Directory Domains	109
Enable Event Stamping in DRA	109
Configure Unified Change History	109
Certificate Validation	110
Access Unified Change History Reports	111
Configuring DRA Services for a Group Managed Service Account	111
Configure the Delegation and Configuration Client	112
Configuring the Web Client	112
Starting the Web Console	113
Auto Logout	113

DRA Server Connection	113
Certificate Validation	114
Authentication	114
12 Connecting Managed Systems	121
Managing Active Directory Domains	121
Adding Managed Domains and Computers	121
Specifying Domain Access Accounts	122
Specifying Exchange Access Accounts	122
Adding a Managed Subtree	123
Adding a Trusted Domain	124
Configuring DRA to Run Secure Active Directory	124
Enable LDAP Over SSL (LDAPS)	124
Configure Automatic Discovery for LDAPS	125
Connecting Public Folders	125
Viewing and Modifying Public Folder Domain Properties	126
Delegating Public Folder Powers	127
Enabling Microsoft Exchange	127
Configuring Azure Tenants	128
Configuring Private Cloud	128
Adding a New Azure Tenant	129
Uploading a Certificate Manually	130
Configuring Certificate-Based Authentication for an Azure Application after Upgrading to 10.2 or later	131
Resetting the Client Secret for an Azure Application	132
Configuring the Azure Guest User Invitation	133
Managing Passwords for Access Accounts	133
Reset Password Manually	133
Schedule a Job to Reset Password	134
Enable LDAP Override Authentication	135
Part V Policy and Process Automation	137
13 Understanding DRA Policy	139
How the Administration Server Enforces Policy	139
Built-in Policy	140
Understanding Built-in Policies	141
Available Policies	141
Using Built-in Policy	143
Implementing a Custom Policy	144
Restricting Native Built-in Security Groups	144
Native Built-in Security Groups You Can Restrict	144
Restricting Actions on Native Built-in Security Groups	145
Managing Policies	146
Microsoft Exchange Policy	146
Office 365 License Policy	148
Creating and Implementing Home Directory Policy	149
Enabling Password Generation	155
Policy Tasks	155
Delegation and Configuration Client Policy	157
Specifying an Automated Mailbox Naming Policy	158

Specifying a Resource Naming Policy	158
Specifying an Archive Naming Policy	158
14 Pre and Post Task Trigger Automation	159
How the Administration Server Automates Processes	159
Implementing an Automation Trigger	160
15 Automated Workflow	163
Part VI Auditing and Reporting	165
16 Auditing Activity	167
Native Windows Event Log	167
Enabling and Disabling Windows Event Log Auditing for DRA	167
Ensuring Auditing Integrity	168
Understanding Log Archives	169
Using the Log Archive Viewer Utility	169
Backing up Log Archive Files	169
Modifying Log Archive Grooming Settings	170
17 Reporting	173
Managing Data Collection for Reporting	173
Viewing the Collectors Status	174
Enabling Reporting and Data Collection	174
Built-in Reports	174
Reporting on Object Changes	175
Reporting on Object Lists	175
Reporting on Object Details	176
Part VII Additional Features	177
18 Temporary Group Assignments	179
19 DRA Dynamic Groups	181
20 How Event Stamping Works	183
The AD DS Event	183
Supported Operations	184
21 BitLocker Recovery Password	185
Viewing and Copying a BitLocker Recovery Password	185
Finding a Recovery Password	185
22 Recycle Bin	187
Assigning Recycle Bin Powers	187

Using the Recycle Bin	187
Part VIII Client Customization	191
23 Delegation and Configuration Client	193
Customizing Property Pages.	193
How Custom Property Pages Work	193
Supported Custom Pages	194
Supported Custom Property Controls	195
Working with Custom Pages	196
Creating Custom Property Pages	197
Modifying Custom Properties.	198
Identifying Active Directory Attributes Managed With Custom Pages	198
Enabling, Disabling, and Deleting Custom Pages	198
Command-Line Interface.	199
Custom Tools	199
Creating Custom Tools.	200
Customizing the User Interface	202
Modifying the Console Title	202
Customizing List Columns	202
24 Web Client	205
Customizing Property Pages.	205
Customizing an Object Property Page	205
Creating a New Object Property Page	206
Customizing Request Forms.	207
Adding Custom Handlers	207
Basic Steps for Creating a Custom Handler	208
Enabling Custom JavaScript	210
Using the Script Editor.	210
About Custom Handler Execution	212
Customizing User Interface Branding	212
Part IX Tools and Utilities	213
25 ActiveView Analyzer Utility	215
Starting an ActiveView Data Collection.	215
Generating an Analyzer Report	216
Identifying the Performance of Objects	217
26 Diagnostic Utility	219
27 Deleted Objects Utility	221
Required Permissions for Deleted Objects Utility	221
Syntax for Deleted Objects Utility	221
Options for Deleted Objects Utility	222
Examples for Deleted Objects Utility.	222

Example 1	222
Example 2	222
Example 3	223
Example 4	223
Example 5	223
28 Health Check Utility	225
29 Recycle Bin Utility	227
Required Permissions for the Recycle Bin Utility	227
Syntax for Recycle Bin Utility	227
Options for Recycle Bin Utility	227
Examples for Recycle Bin Utility	228
Example 1	228
Example 2	228
Example 3	228
A Appendix	229
DRA Services	229
Troubleshooting DRA REST Services	230
Handling Certificates for the DRA REST Extensions	230
Handling Errors from the DRA Server	231
Every PowerShell Command Results in PSInvalidOperation Error	232
WCF Trace Logging	232
Troubleshooting Installation and Upgrade	233
Pre-requisites are missing error when you manage an Azure tenant	233
Troubleshooting Installation Issues with Microsoft.graph Version 2.9	233

About this Guide

The *Administrator Guide* provides conceptual information about the NetIQ Directory and Resource Administrator (DRA) product. This book defines terminology and various related concepts. It also provides step-by-step guidance for many configuration and operational tasks.

Intended Audience

This book provides information for individuals responsible for understanding administration concepts and implementing a secure, distributed administration model.

Additional Documentation

This guide is part of the Directory and Resource Administrator documentation set. For the most recent version of this guide and other DRA documentation resources, visit the [DRA Documentation website](#).

Contact Information

We want to hear your comments and suggestions about this book and the other documentation included with this product. You can use the [comment on this topic](#) link at the bottom of each page of the online documentation, or send an email to MFI-Documentation-Feedback@opentext.com.

For specific product issues, contact Open Text Support for Micro Focus products at <https://www.microfocus.com/support-and-services/>.

Getting Started

Before you install and configure all the components of Directory and Resource Administrator™ (DRA) you should understand the basic tenets of what DRA will do for your enterprise and the role of DRA components in the product architecture.

- ♦ [Chapter 1, “What is Directory and Resource Administrator,” on page 15](#)
- ♦ [Chapter 2, “Understanding Directory and Administrator Components,” on page 17](#)

1 What is Directory and Resource Administrator

Directory and Resource Administrator delivers secure and efficient privileged-identity administration of Microsoft Active Directory (AD). DRA performs granular delegation of “least privilege” so that administrators and users receive just the permissions needed to complete their specific responsibilities. DRA also enforces adherence to policy, provides detailed-activity auditing and reporting, and simplifies repetitive task completion with IT process automation. Each of these capabilities contributes to protecting your customers’ AD and Exchange environments from the risk of privilege escalation, errors, malicious activity, and regulatory non-compliance, while reducing administrator burden by granting self-service capabilities to users, business managers and Help Desk personnel.

DRA also extends the powerful features of Microsoft Exchange to provide seamless management of Exchange objects. Through a single, common user interface, DRA delivers policy-based administration for the management of mailboxes, public folders, and distribution lists across your Microsoft Exchange environment.

DRA provides the solutions you need to control and manage your Microsoft Active Directory, Windows, Exchange, and Azure Active Directory environments.

- ◆ **Support for Azure and on-premises Active Directory, Exchange, and Skype for Business:**

Delivers administrative management of Azure and on-premises Active Directory, on-premises Exchange Server, on-premises Skype for Business, and Exchange Online.

- ◆ **Granular user and administrative privilege-access controls:** Patented ActiveView technology delegates just the privileges needed to complete specific responsibilities and protect against privilege escalation.
- ◆ **Customizable web console:** Intuitive approach enables non-technical personnel to perform administrative tasks easily and safely through limited (and assigned) capabilities and access.
- ◆ **In-depth activity auditing and reporting:** Provides a comprehensive audit record of all activity performed with the product. Securely stores long-term data and demonstrates to auditors (e.g., PCI DSS, FISMA, HIPAA and NERC CIP) that processes are in place for controlling access to AD.
- ◆ **IT Process Automation:** Automates workflows for a variety of tasks, like provisioning and deprovisioning, user and mailbox actions, policy enforcement, and controlled self-service tasks; increases business efficiencies, and reduces manual and repetitive administrative efforts.
- ◆ **Operational integrity:** Prevents malicious or incorrect changes that affect the performance and availability of systems and services by providing granular access control for administrators and managing access to systems and resources.
- ◆ **Process enforcement:** Maintains the integrity of key change management processes that help you improve productivity, reduce errors, save time, and increase administration efficiency.
- ◆ **Integration with Change Guardian:** Enhances auditing for events generated in Active Directory outside of DRA and workflow automation.

2 Understanding Directory and Administrator Components

The components of DRA that you will consistently use to manage privileged access include primary and secondary servers, administrator consoles, reporting components, and the Workflow Automation Engine to automate workflow processes.

The following table identifies the typical user interfaces and Administration servers used by each type of DRA user:

Type of DRA User	User Interfaces	Administration Server
DRA Administrator (The person who will maintain the product configuration)	Delegation and Configuration Console	Primary server
Advanced Administrator	DRA Reporting Center Setup (NRC) PowerShell <i>(optional)</i> CLI <i>(optional)</i> DRA ADSI Provider <i>(optional)</i>	Any DRA server
Help Desk Occasional Administrator	Web Console	Any DRA server

DRA Administration Server

The DRA Administration server stores configuration data (environmental, delegated access, and policy), executes operator and automation tasks, and audits system-wide activity. While supporting several console and API level clients, the server is designed to provide high availability for both redundancy and geographic isolation through a Multi-Master Set (MMS) scale-out model. In this model, every DRA environment will require one primary DRA Administration server that will synchronize with additional secondary DRA Administration servers.

We strongly recommend that you do not install Administration servers on Active Directory domain controllers. For each domain that DRA manages, ensure there is at least one domain controller in the same site as the Administration server. By default, the Administration server accesses the closest domain controller for all read and write operations; when performing site-specific tasks, such as password resets, you can specify a site-specific domain controller to process the operation. As a best practice, consider dedicating a secondary Administration server for your reporting, batch processing, and automated workloads.

Delegation and Configuration Console

The Delegation and Configuration console is an installable user interface that provides system administrators access to DRA configuration and administration functions.

- ♦ **Delegation Management:** Enables you to granularly specify and assign access to managed resources and tasks to assistant administrators.
- ♦ **Policy and Automation Management:** Enables you to define and enforce policy to ensure compliance with the standards and conventions of the environment.
- ♦ **Configuration Management:** Enables you to update DRA system settings and options, add customizations, and configure managed services (Active Directory, Exchange, Azure Active Directory, etc.).
- ♦ **Account and Resource Management:** Enables DRA assistant administrators to view and manage delegated objects of connected domains and services from the Delegation and Configuration Console.

Web Console

The Web Console is a web-based user interface that provides quick and easy access to assistant administrators to view and manage delegated objects of connected domains and services. Administrators can customize the look and use of the Web Console to include customized enterprise branding and customized object properties.

Reporting Components

DRA Reporting provides built-in, customizable templates for DRA management and details of DRA managed domains and systems:

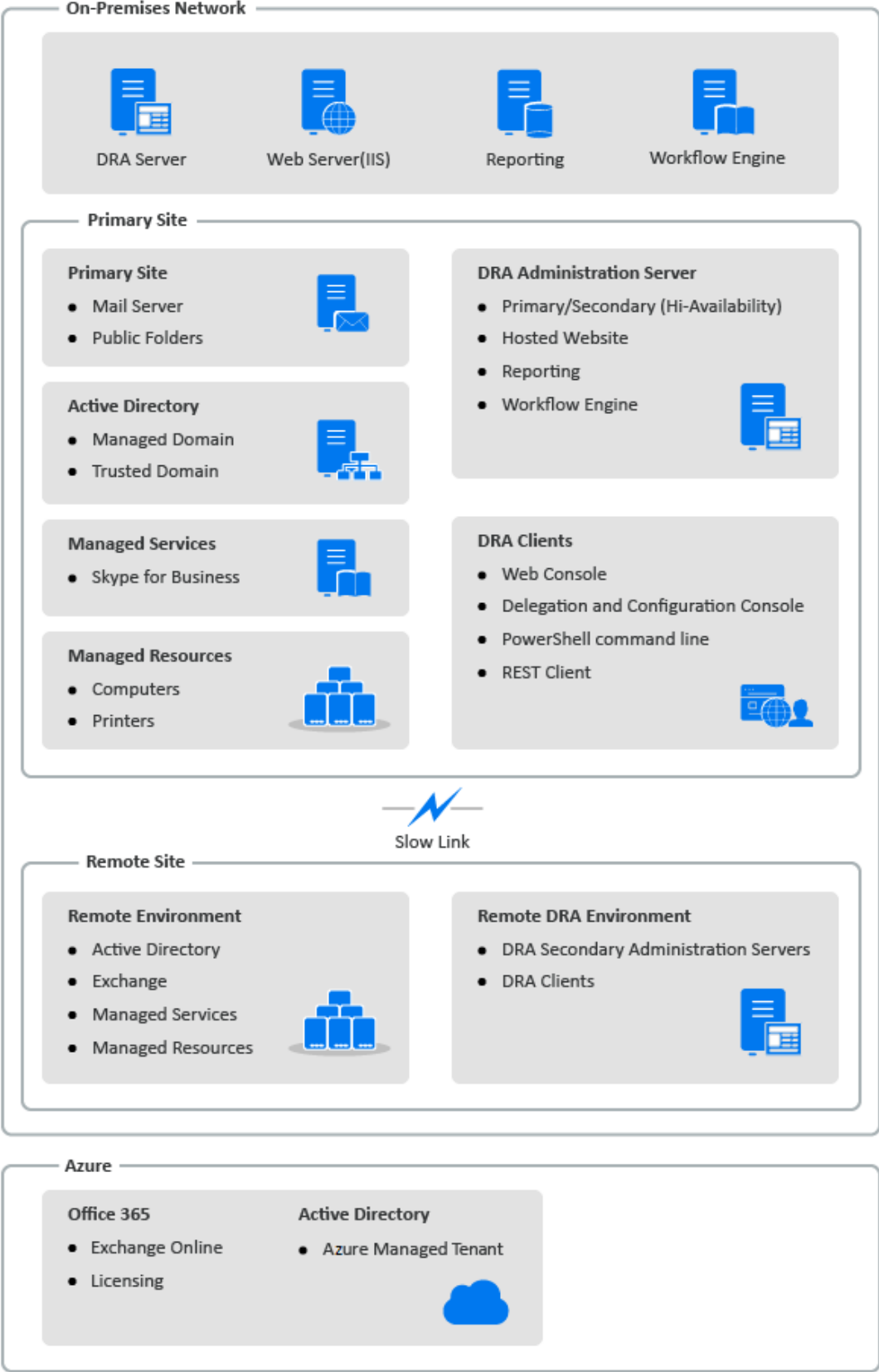
- ♦ Resources reports for Active Directory objects
- ♦ Active Directory object data reports
- ♦ Active Directory summary reports
- ♦ DRA configuration reports
- ♦ Exchange configuration reports
- ♦ Office 365 Exchange Online reports
- ♦ Detailed activity trends reports (By month, domain, and peak)
- ♦ Summarized DRA activity reports

DRA reports can be scheduled and published through SQL Server Reporting Services for convenient distribution to stakeholders.

Workflow Automation Engine

DRA integrates with the Workflow Automation Engine to automate workflow tasks via the Web Console where assistant administrators can configure the Workflow Server and execute customized workflow automation forms, and then view the status of those workflows. For more information about the Workflow Automation Engine, see the [DRA Documentation site](#).

Product Architecture





Product Installation and Upgrade

This chapter outlines the recommended hardware, software, and account requirements required by Directory and Resource Administrator. It then guides you through the installation process with a checklist for each component of the installation.

- ♦ [Chapter 3, “Planning Your Deployment,” on page 23](#)
- ♦ [Chapter 4, “Product Installation,” on page 41](#)
- ♦ [Chapter 5, “Product Upgrade,” on page 47](#)

3 Planning Your Deployment

As you plan your Directory and Resource Administrator deployment, use this section to assess your hardware and software environment for compatibility and to note the required ports and protocols you will need to configure for the deployment.

- ♦ [“Tested Resource Recommendations” on page 23](#)
- ♦ [“Virtual Environment Resource Provisioning” on page 23](#)
- ♦ [“Required Ports and Protocols” on page 24](#)
- ♦ [“Supported Platforms” on page 27](#)
- ♦ [“DRA Administration Server and Web Console Requirements” on page 29](#)
- ♦ [“Reporting Requirements” on page 37](#)
- ♦ [“Licensing Requirements” on page 38](#)
- ♦ [“Language Support” on page 38](#)

Tested Resource Recommendations

This section provides sizing information for our base resource recommendation. Your results may vary based on the hardware available, the specific environment, the specific type of data processed, and other factors. It is likely that larger, more powerful hardware configurations exist that can handle a greater load. If you have questions, please consult with Consulting Services.

Executed in an environment with approximately one million Active Directory objects:

Component	CPU	Memory	Storage
DRA Administration Server	8 CPU/cores 2.0 GHz	16 GB	120 GB
DRA Web Console	2 CPU/cores 2.0 GHz	8 GB	100 GB
DRA Reporting	4 CPU/cores 2.0 GHz	16 GB	100 GB
DRA Workflow Server	4 CPU/cores 2.0 GHz	16 GB	120 GB

Virtual Environment Resource Provisioning

DRA keeps large memory segments active for extended period of time. When provisioning resources for a virtual environment, the following recommendations should be considered:

- ♦ Allocate the storage as “Thick Provisioned”
- ♦ Set memory reservation to Reserve All Guest Memory (All Locked)
- ♦ Make sure that the paging file is large enough to cover the potential ballooned memory reallocation at the virtual layer

Required Ports and Protocols

The ports and protocols for DRA communication are provided in this section.

- ◆ Configurable ports are indicated with one asterisk *
- ◆ Ports requiring a certificate are indicated with two asterisks **

Component tables:

- ◆ [“DRA Administration Servers” on page 24](#)
- ◆ [“DRA REST Server” on page 26](#)
- ◆ [“Web Console \(IIS\)” on page 26](#)
- ◆ [“DRA Delegation and Administration Console” on page 26](#)
- ◆ [“Workflow Server” on page 27](#)

DRA Administration Servers

Protocol and Port	Direction	Destination	Usage
TCP 135	Bi-directional	DRA Administration Servers	End-point mapper, a basic requirement for DRA communication; enables Administration servers to locate each other in MMS
TCP 445	Bi-directional	DRA Administration Servers	Delegation model replication; file replication during MMS synchronization (SMB)
Dynamic TCP port range *	Bi-directional	Microsoft Active Directory domain controllers	By default, DRA assigns ports dynamically from the TCP port range of 1024 through 65535. You can, however, configure this range by using Component Services. For more information, see Using Distributed COM with Firewalls .
TCP 50000 *	Bi-directional	DRA Administration Servers	Attribute replication and DRA server-AD LDS communication. (LDAP)
TCP 50001 *	Bi-directional	DRA Administration Servers	SSL attribute replication (AD LDS)
TCP/UDP 389	Outbound	Microsoft Active Directory domain controllers	Active Directory object management (LDAP)
	Outbound	Microsoft Exchange Server	Mailbox management (LDAP)
TCP/UDP 53	Outbound	Microsoft Active Directory domain controllers	Name resolution

Protocol and Port	Direction	Destination	Usage
TCP/UDP 88	Outbound	Microsoft Active Directory domain controllers	Allows authentication from the DRA Server to the domain controllers (Kerberos)
TCP 80	Outbound	Microsoft Exchange Server	Needed for all on-premises Exchange servers 2016 and later (HTTP)
	Outbound	Microsoft Office 365	Remote PowerShell access (HTTP)
TCP 443	Outbound	Microsoft Office 365, Change Guardian	Graph API access and Change Guardian Integration (HTTPS)
TCP 443, 5986, 5985	Outbound	Microsoft PowerShell	Native PowerShell cmdlets (HTTPS) and PowerShell Remoting
TCP 5984	Localhost	DRA Administration Servers	IIS access to the Replication Service to support temporary group assignments
TCP 8092 * **	Outbound	Workflow Server	Workflow status and triggering (HTTPS)
TCP 50101 *	Inbound	DRA Client	Right-Click Change History report to UI Audit Report. Can be configured during installation.
TCP 8989	Localhost	Log Archive Service	Log archive communication (does not need to be opened through the firewall)
TCP 50102	Bi-directional	DRA Core Service	Log Archive Service
TCP 50103	Localhost	DRA Cache DB Service	Cache service communication on the DRA server (does not need to be opened through the firewall)
TCP 1433	Outbound	Microsoft SQL Server	Reporting data collection
UDP 1434	Outbound	Microsoft SQL Server	SQL Server browser service uses this port to identify the port for the named instance.
TCP 8443	Bi-directional	Change Guardian Server	Unified Change History
TCP 8898	Bi-directional	DRA Administration Servers	DRA Replication Service communication between DRA servers for temporary group assignments
TCP 636	Outbound	Microsoft Active Directory domain controllers	Active Directory object management (LDAP SSL).

DRA REST Server

Protocol and Port	Direction	Destination	Usage
TCP 8755 * **	Inbound	IIS Server, DRA PowerShell cmdlets	Execute DRA REST-based workflow activities (ActivityBroker)
TCP 135	Outbound	Microsoft Active Directory domain controllers	Autodiscovery using Service Connection Point (SCP)
TCP 443	Outbound	Microsoft AD Domain Controllers	Autodiscovery using Service Connection Point (SCP)

Web Console (IIS)

Protocol and Port	Direction	Destination	Usage
TCP 8755 * **	Outbound	DRA REST Service	For communication between DRA Web Console, and DRA PowerShell
TCP 443	Inbound	Client Browser	Opening a DRA website
TCP 443 **	Outbound	Advanced Authentication Server	Advanced Authentication

DRA Delegation and Administration Console

Protocol and Port	Direction	Destination	Usage
TCP 135	Outbound	Microsoft Active Directory domain controllers	Autodiscovery using SCP
Dynamic TCP port range *	Outbound	DRA Administration Servers	DRA Adapter workflow activities. By default, DCOM assigns ports dynamically from the TCP port range of 1024 through 65535. You can, however, configure this range by using Component Services. For more information, see Using Distributed COM with Firewalls (DCOM)
TCP 50102	Outbound	DRA Core Service	Change History report generation

Workflow Server

Protocol and Port	Direction	Destination	Usage
TCP 8755	Outbound	DRA Administration Servers	Execute DRA REST-based workflow activities (ActivityBroker)
Dynamic TCP port range *	Outbound	DRA Administration Servers	DRA Adapter workflow activities. By default, DCOM assigns ports dynamically from the TCP port range of 1024 through 65535. You can, however, configure this range by using Component Services. For more information, see Using Distributed COM with Firewalls (DCOM)
TCP 1433	Outbound	Microsoft SQL Server	Workflow data storage
TCP 8091	Inbound	Operations Console and Configuration Console	Workflow BSL API (TCP)
TCP 8092 **	Inbound	DRA Administration Servers	Workflow BSL API (HTTP) and (HTTPS)
TCP 2219	Localhost	Namespace Provider	Used by the Namespace Provider to run adapters
TCP 9900	Localhost	Correlation Engine	Used by the Correlation Engine to communicate with the Workflow Automation Engine and Namespace Provider
TCP 10117	Localhost	Resource Management Namespace Provider	Used by the Resource Management Namespace Provider

Supported Platforms

For information about supported software platforms, refer to the [Directory and Resource Administrator product page](#).

Managed System	Prerequisites
Azure Active Directory	<p>To enable Azure administration, you must install the following PowerShell modules:</p> <p>DRA 10.2.3:</p> <ul style="list-style-type: none"> ◆ Microsoft.Graph 2.8 or later ◆ Exchange Online PowerShell V3.0.0 or later ◆ Az.Accounts 1.2.1 or later <p>DRA 10.2.2 or earlier:</p> <ul style="list-style-type: none"> ◆ Azure Active Directory V2 (AzureAD) 2.0.2.4 version or later ◆ Exchange Online PowerShell V2.0.3 or later ◆ Az.Accounts 1.2.1 or later <p>IMPORTANT</p> <ul style="list-style-type: none"> ◆ Beginning with DRA 10.2.1, the Az.Accounts module replaces the AzureRM.Profile module. If you are upgrading from an earlier version of DRA, you can retain the existing AzureRM.Profile module if necessary, and install the Az.Accounts module using the -AllowClobber parameter in the Install-Module cmdlet. ◆ If FIPS is enabled, the prerequisites check does not recognize the installed PowerShell modules. To ensure that the prerequisites check is successful, turn off FIPS. <p>PowerShell 5.1 or the latest module is required to install the new Azure PowerShell modules.</p>
Active Directory	<ul style="list-style-type: none"> ◆ Microsoft Windows Server 2012 R2 ◆ Microsoft Windows Server 2016 ◆ Microsoft Windows Server 2019 ◆ Microsoft Windows Server 2022 ◆ Azure Active Directory
Microsoft Exchange	<ul style="list-style-type: none"> ◆ Microsoft Exchange 2016 ◆ Microsoft Exchange 2019
Microsoft Office 365	<ul style="list-style-type: none"> ◆ Microsoft Exchange Online O365
Skype for Business	<ul style="list-style-type: none"> ◆ Microsoft Skype for Business 2015
Change History	<ul style="list-style-type: none"> ◆ Change Guardian 6.3
Databases	<ul style="list-style-type: none"> ◆ Microsoft SQL Server 2016 ◆ Microsoft SQL Server 2019 ◆ Microsoft SQL Server 2022
Web Browsers	<ul style="list-style-type: none"> ◆ Google Chrome ◆ Mozilla Firefox ◆ Microsoft Edge

Managed System	Prerequisites
Workflow Automation	<ul style="list-style-type: none"> ◆ Microsoft Windows Server 2016 ◆ Microsoft Windows Server 2019 ◆ Microsoft Windows Server 2022

DRA Administration Server and Web Console Requirements

DRA components require the following software and accounts:

- ◆ [“Software Requirements” on page 29](#)
- ◆ [“Server Domain” on page 31](#)
- ◆ [“Account Requirements” on page 31](#)
- ◆ [“Least Privilege DRA Access Accounts” on page 33](#)

Software Requirements

Component	Prerequisites
Installation Target	Administration Server Operating System:
Operating System	<ul style="list-style-type: none"> ◆ Microsoft Windows Server 2016, 2019, 2022 <p>NOTE: The server must also be a member of a supported Microsoft on-premises Active Directory domain.</p> <p>DRA Interfaces:</p> <ul style="list-style-type: none"> ◆ Microsoft Windows Server 2016, 2019, 2022 ◆ Microsoft Windows 10, 11
Installer	<ul style="list-style-type: none"> ◆ Microsoft .Net Framework 4.8 and above

Component	Prerequisites
Administration Server	<p data-bbox="678 220 1101 247">Directory and Resource Administrator:</p> <ul data-bbox="704 275 1409 667" style="list-style-type: none"> ◆ Microsoft .Net Framework 4.8 and above ◆ Microsoft Visual C++ 2015-2019 Redistributable Packages (x64 and x86) ◆ Microsoft Message Queuing ◆ Microsoft Active Directory Lightweight Directory Services roles ◆ Remote Registry Service Started ◆ Microsoft Internet Information Services ◆ Microsoft Internet Information Services URL Rewrite Module ◆ Microsoft Internet Information Services application request routing <p data-bbox="678 695 1325 753">NOTE: DRA REST Endpoint and Service are installed with the Administration Server.</p> <p data-bbox="678 781 1276 808">Microsoft Office 365/Exchange Online Administration:</p> <p data-bbox="678 835 805 863">DRA 10.2.3:</p> <ul data-bbox="704 890 1198 1045" style="list-style-type: none"> ◆ Windows PowerShell Module ◆ Microsoft.Graph 2.8 or later ◆ Az.accounts 1.2.1 or later ◆ Exchange Online PowerShell V3.0.0 or later <p data-bbox="678 1073 911 1100">DRA 10.2.2 or earlier:</p> <ul data-bbox="704 1127 1442 1329" style="list-style-type: none"> ◆ Windows PowerShell Module ◆ Windows Azure Active Directory Module for Windows PowerShell ◆ Exchange Online PowerShell V2.0.3 or later ◆ Enable WinRM for Basic authentication on the client-side for Exchange Online tasks. <p data-bbox="678 1356 1195 1383">For more information, see Supported Platforms.</p>
User Interface	<p data-bbox="678 1409 850 1436">DRA Interfaces:</p> <ul data-bbox="704 1463 1409 1564" style="list-style-type: none"> ◆ Microsoft .Net Framework 4.8 ◆ Microsoft Visual C++ 2015-2019 Redistributable Packages (x64 and x86)
PowerShell Extensions	<ul data-bbox="704 1591 1057 1661" style="list-style-type: none"> ◆ Microsoft .Net Framework 4.8 ◆ PowerShell 5.1 or later

Component	Prerequisites
DRA Web Console	<p>Web Server:</p> <ul style="list-style-type: none"> ◆ Microsoft .Net Framework 4.x > WCF Services > HTTP Activation ◆ Microsoft Internet Information Server 8.5, 10 ◆ Microsoft Internet Information Services URL Rewrite Module ◆ Microsoft Internet Information Services application request routing <p>Web Server (IIS) components:</p> <ul style="list-style-type: none"> ◆ Web Server > Security > URL Authorization

Server Domain

Component	Operating Systems
DRA Server	<ul style="list-style-type: none"> ◆ Microsoft Windows Server 2022 ◆ Microsoft Windows Server 2019 ◆ Microsoft Windows Server 2016

Account Requirements

Account	Description	Permissions
AD LDS Group	The DRA service account needs to be added to this group for access to AD LDS	<ul style="list-style-type: none"> ◆ Domain Local Security Group

Account	Description	Permissions
DRA Service Account	The permissions required to run the Administration Service	<ul style="list-style-type: none"> ◆ “Distributed COM Users” Permissions ◆ Member of the AD LDS Admin Group ◆ Account Operator Group ◆ Log Archive groups (OnePointOp ConfgAdms & OnePointOp) ◆ When installing DRA on a server using STIG methodology, select one of the following options for the DRA service account user from the User account flags area of the Accounts tab on the user properties page: <ul style="list-style-type: none"> ◆ This account supports Kerberos AES 128 bits encryption ◆ This account supports Kerberos AES 256 bits encryption
NOTE		
		<ul style="list-style-type: none"> ◆ For more information about setting up least privilege domain access accounts see, Least Privilege DRA Access Accounts. ◆ For more information on setting up a group Managed Service Account for DRA see, “Configuring DRA Services for a Group Managed Service Account” in the <i>DRA Administrator Guide</i>.
DRA Administrator	User account or Group provisioned to the built-in DRA Admins role	<ul style="list-style-type: none"> ◆ Domain Local Security Group or domain user account ◆ Member of the managed domain or a trusted domain <ul style="list-style-type: none"> ◆ If you specify an account from a trusted domain, ensure that the Administration server computer can authenticate this account.

Account	Description	Permissions
DRA Assistant Admin Accounts	Accounts that get delegated powers through DRA	<ul style="list-style-type: none"> ◆ Add all DRA Assistant Admin accounts to the “Distributed COM Users” group so that they can connect to the DRA Server from remote clients. It is required only when you are using a thick client or the Delegation and Configuration console. <p>NOTE: DRA can be configured to manage this for you during the installation.</p>

Least Privilege DRA Access Accounts

A DRA access account allows you to override the Administration service account you configured for the Administration server when you installed DRA. These accounts can be used to access domains, tenants, public folders and so on. The following sections list the permissions and privileges that are required for the access accounts and the configuration commands you need to run.

Domain Access Account: Using ADSI Edit, grant the Domain Access account the following Active Directory Permissions at the top domain level:

1. Launch ADSI Edit.
2. Select the domain node (DC=<Domain_Name>,DC=/?), right-click and select **Properties**.
3. Click **Security > Advanced > Permissions**.
4. Select the domain access account and click **Edit**.
5. Ensure that the **Type** list is set to Allow.
6. In the **Applies to** list, select `Descendant builtInDomain` objects.
7. Under **Permissions**, select the `Full Control` check box.
8. Repeat steps 6-7, and provide Full control for the following descendant objects:
 - ◆ Descendant Computer objects
 - ◆ Descendant Connection Point objects
 - ◆ Descendant Contact objects
 - ◆ Descendant Container objects
 - ◆ Descendant Group objects
 - ◆ Descendant InetOrgPerson objects
 - ◆ Descendant MsExchDynamicDistributionList objects
 - ◆ Descendant MsExchSystemObjectsContainer objects
 - ◆ Descendant msDS-GroupManagedServiceAccount objects
 - ◆ Descendant Organizational Unit objects
 - ◆ Descendant Printer objects
 - ◆ Descendant publicFolder objects

- ◆ Descendant Shared Folder objects
 - ◆ Descendant User objects
9. With the **Type** list set to Allow, select **This object** and all descendant objects from the **Applies to** list.
10. Under **Permissions**, select the following check boxes:
- ◆ Create Computer objects
 - ◆ Delete Computer objects
 - ◆ Create Contact objects
 - ◆ Delete Contact objects
 - ◆ Create Container objects
 - ◆ Delete Container objects
 - ◆ Create Group objects
 - ◆ Delete Group objects
 - ◆ Delete InetOrgPerson objects
 - ◆ Create MsExchDynamicDistributionList objects
 - ◆ Delete MsExchDynamicDistributionList objects
 - ◆ Create msDS-GroupManagedServiceAccount objects
 - ◆ Delete msDS-GroupManagedServiceAccount objects
 - ◆ Create Organizational Unit objects
 - ◆ Delete Organizational Unit objects
 - ◆ Create publicFolders objects
 - ◆ Delete publicFolders objects
 - ◆ Create Shared Folder objects
 - ◆ Delete Shared Folder objects
 - ◆ Create User objects
 - ◆ Delete User objects
 - ◆ Create Printer objects
 - ◆ Delete Printer objects
11. Click **OK**.

Using ADSI Edit, provide read access to the Microsoft Exchange container for the Domain Access account by following these steps:

1. Launch ADSI Edit (adsiedit.msc).
2. In the left navigation pane, right-click ADSI Edit and choose **Connect to**.
3. Select Configuration as the well-known Naming Context, then click **OK**.
4. Expand the Configuration node. (CN=Configuration,DC=<Domain_Name>,DC=/?).
5. Navigate to CN=services -> CN=Microsoft Exchange.
6. Right-click CN=Microsoft Exchange and select **Properties**.
7. Click **Security>Advanced>Permissions**.

8. Locate the domain access account then click **Edit**.
9. Confirm that the **Type** list is set to Allow.
10. In the **Applies to** list, select Descendant objects.
11. Under **Permissions**, select List Contents, Read all Properties and Read Permissions check box.
12. Click OK and then Apply.

NOTE

- ◆ If the managed domain's Active Directory schema is not extended for Exchange Online, the following objects will not be listed:
 - ◆ MsExchDynamicDistributionList objects
 - ◆ MsExchSystemObjectsContainer objects
 - ◆ publicFolder objects
- ◆ By default, some Built-in container objects within Active Directory do not inherit permissions from the top level of the domain. For this reason, those objects will require inheritance to be enabled, or explicit permissions to be set.
- ◆ If you use the least privilege account as the access account, ensure that the account is assigned the "Reset Password" permission for itself in Active Directory for the password reset to be successful in DRA.

Exchange Access Account: To manage on-premises Microsoft Exchange objects, assign the Organizational Management role to the Exchange Access Account and the Exchange Access Account to the Account Operators group.

Skype Access Account: Ensure that this account is a Skype-enabled user and that is a member of at least one of the following:

- ◆ CSAdministrator role
- ◆ Both the CSUserAdministrator and CSArchiving roles

Public Folder Access Account: Assign the following Active Directory permissions to the Public Folder Access Account:

- ◆ Public Folder Management
- ◆ Mail Enabled Public Folders

Azure Tenant: Basic authentication requires Azure Active Directory permissions on both the Azure Tenant Access Account and the Azure application. Certificate-based authentication requires Azure Active Directory permissions on the Azure application. By default, DRA automatically creates a self-signed certificate required for authentication.

Azure application: The Azure application requires the following roles and permissions:

Roles:

- ◆ User administrator
- ◆ Exchange administrator

Permissions:

- ◆ Read and write all users' full profiles
- ◆ Read and write all groups
- ◆ Read directory data
- ◆ Manage Exchange Online as an application to access Exchange Online resources
- ◆ Read and write all applications
- ◆ Exchange Recipient Administrator

Azure Tenant Access Account: The Azure Tenant Access Account requires the following permissions:

- ◆ Distribution Groups
- ◆ Mail Recipients
- ◆ Mail Recipient Creation
- ◆ Security Group Creation and Membership
- ◆ (Optional) Skype for Business Administrator

If you want to manage Skype for Business Online, assign the Skype for Business Administrator power to the Azure tenant access account.

- ◆ User Administrator
- ◆ Privileged authentication administrator

Administration Service Account Permissions:

- ◆ Local Administrators
- ◆ Grant the least privilege override account “Full Permission” on share folders or DFS folders where Home directories are provisioned.
- ◆ **Resource Management:** To manage published resources within a managed Active Directory domain, the Domain Access account must be granted local administration permissions on those resources.

Post DRA installation: You must run the following commands before you manage the required domains:

- ◆ To delegate permission to the “Deleted Objects Container” from the DRA Installation folder (Note: the command must be executed by a domain administrator):

```
DraDelObjsUtil.exe /domain:<NetbiosDomainName> /delegate:<Account Name>
```

- ◆ To delegate permission to the “NetIQRecycleBin OU” from the DRA Installation folder:

```
DraRecycleBinUtil.exe /domain:<NetbiosDomainName> /  
delegate:<AccountName>
```

Remote Access to SAM: Assign Domain Controllers or member servers managed by DRA to enable the accounts listed in the GPO setting below, so they can make remote queries to the Security Account Manager's (SAM) database. The configuration needs to include the DRA service account.

Network access: Restrict clients allowed to make remote calls to SAM

To access this setting, do the following:

- 1 Open the Group Policy Management console on the domain controller.
- 2 Expand **Domains > [domain controller] > Group Policy Objects** in the node tree.
- 3 Right-click **Default Domain Controllers Policy** and select **Edit** to open the GPO editor for this policy.
- 4 Expand **Computer Configuration > Policies > Windows Settings > Security Settings > Local Policies** in the node tree of the GPO editor.
- 5 Double-click **Network access: Restrict clients allowed to make remote calls to SAM** in the policies pane, and select **Define this policy setting**.
- 6 Click **Edit Security** and enable **Allow** for Remote Access. Add the DRA service account if it is not already included as a user or part of the administrators group.
- 7 Apply the changes. This will add the security descriptor, `O : BAG : BAD : (A ; ; RC ; ; BA)` to the policy settings.

For more information, see [Knowledge Base article 7023292](#).

Reporting Requirements

Requirements for the DRA Reporting include the following:

Software Requirements

Component	Prerequisites
Installation Target	Operating System: <ul style="list-style-type: none">◆ Microsoft Windows Server 2016, 2019, 2022
Reporting Center (v3.3.2)	Database: <ul style="list-style-type: none">◆ Microsoft SQL Server 2016◆ Microsoft SQL Server 2019◆ Microsoft SQL Server 2022◆ Microsoft SQL Server Reporting Services◆ The Domain administrator who manages SQL Agent jobs requires security permissions for Microsoft SQL Server Integration Services or some NRC reports may not be processed. Web Server: <ul style="list-style-type: none">◆ Microsoft Internet Information Server 10◆ Microsoft IIS Components:<ul style="list-style-type: none">◆ ASP .NET 4.0 and later <p>SQL Server must have an updated TLS supported driver installed on the DRA server.</p>

Component	Prerequisites
DRA Reporting	Database: <ul style="list-style-type: none"> ◆ Microsoft SQL Server Integration Services ◆ Microsoft SQL Server Agent

Licensing Requirements

Your license determines the products and features you can use. DRA requires a license key installed with the Administration Server.

After you install the Administration server, you can use the Health Check Utility to install your purchased license. A trial license key (TrialLicense.lic) is also included in the installation package that enables you to manage an unlimited number of user accounts and mailboxes for 30 days. For more information about DRA licenses, see [Installing or Upgrading Licenses](#).

Refer to the product End User License Agreement (EULA) for additional information regarding license definition and restrictions.

Language Support

1. Web Browser Language Localization:

DRA supports language localization as part of the Web Browser and when the web browser is running on a localized operating system.

DRA supports localization in the following languages:

- ◆ English (US)
- ◆ French
- ◆ French (Canada)
- ◆ German
- ◆ Italian
- ◆ Japanese
- ◆ Portuguese
- ◆ Spanish
- ◆ Chinese
- ◆ Chinese (Taiwan)

2. Localized Character Support for Object Names:

DRA supports AD attribute names and values containing characters found within the standard ASCII character set.

3. DRA Installation in Non-English Localized Operating System:

DRA's installer is in English.

4. Windows Domain Controllers with Full Localization:

DRA is expected to work with Windows Domain Controllers that operate in a fully localized environment, provided that object names in Active Directory conform to the standard ASCII character set.

4 Product Installation

This chapter guides you through installing the Directory and Resource Administrator. For more information on planning your install or upgrade, see [Planning Your Deployment](#).

- ◆ “Install the DRA Administration Server” on page 41
- ◆ “Install DRA Clients” on page 43
- ◆ “Install Workflow Automation and Configure Settings” on page 44
- ◆ “Install DRA Reporting” on page 44

Install the DRA Administration Server

You can install the DRA Administration Server as either a primary or secondary node in your environment. The requirements for a primary and secondary administration server are the same, however, every DRA deployment must include one primary administration server.

The DRA server package has the following features:

- ◆ **Administration Server:** Stores configuration data (environmental, delegated access, and policy), executes operator and automation tasks, and audits system-wide activity. It has the following features:
 - ◆ **Log Archive Resource Kit:** Enables you to view audit information.
 - ◆ **DRA SDK:** Provides the ADSI sample scripts and helps you to create your scripts.
 - ◆ **Temporary Group Assignments:** Provides the components to enable synchronization of Temporary Group Assignments.
- ◆ **User Interfaces:** The web client interface that is primarily used by assistant administrators, but also includes customization options.
 - ◆ **ADSI Provider:** Enables you to create policy scripts.
 - ◆ **Command-line Interface:** Enables you to perform DRA operations.
 - ◆ **Delegation and Configuration:** Enable system administrators access to DRA configuration and administration functions. Also, enables you to granularly specify and assign access to managed resources and tasks to assistant administrators.
 - ◆ **PowerShell Extensions:** Provides a PowerShell module that allows non-DRA clients to request DRA operations using PowerShell cmdlets.
 - ◆ **Web Console:** The web client interface that is primarily used by assistant administrators, but also includes customization options.

For information about installing specific DRA consoles and command line clients on multiple computers, see [Install the DRA Clients](#).

Interactive Installation Checklist:

Step	Details
Log on to the target server	Log on to the target Microsoft Windows server for the install with an account that has local administrative privileges.
Copy and run the Admin Installation Kit	Execute the DRA installation kit (NetIQAdminInstallationKit.msi) to extract the DRA installation media to the local file system. NOTE: The installation kit will install the .Net framework on the target server if needed.
Install DRA	Click Install DRA and Next to see the installation options. NOTE: To run the install later, navigate to the location where the installation media was extracted (View Installation Kit), and execute <code>Setup.exe</code> .
Default Installation	Choose the components to install and either accept the default installation location <code>C:\Program Files (x86)\NetIQ\DRA</code> or specify an alternate location for the installation. Component options: Administration Server <ul style="list-style-type: none">◆ Log Archive Resource Kit (Optional)◆ DRA SDK◆ Temporary Group Assignments User Interfaces <ul style="list-style-type: none">◆ ADSI Provider (Optional)◆ Command-line Interface (Optional)◆ Delegation and Configuration◆ PowerShell Extensions◆ Web Console
Verify prerequisites	The Prerequisites List page displays a list of required software based on the components selected for the installation. The installer will guide you through installing any missing prerequisites that are required for the install to complete successfully.
Accept the EULA license agreement	Accept the terms of the End User License Agreement.
Specify log location	Specify a location for DRA to store all the log files. NOTE: The Delegation and Configuration Console logs and ADSI logs are stored in the user-profile folder.
Select the Server Operation Mode	Select Primary Administration Server to install the first DRA Administration Server in a multi-master set (there will be only one primary in a deployment) or Secondary Administration Server to join a new DRA Administration Server to an existing multi-master set. For information about multi-master set, see “Configuring the Multi-Master Set” in the <i>DRA Administrator Guide</i> .

Step	Details
Specify installation accounts and credentials	<ul style="list-style-type: none"> ◆ DRA Service Account ◆ AD LDS Group ◆ DRA Administrator Account <p>For more information see, DRA Administration Server and Web Console Requirements.</p>
Configure DCOM permissions	Enable DRA to configure “Distributed COM” access to authenticated users.
Configure ports	For more information on the default ports, see Required Ports and Protocols .
Specify storage location	Specify the local file location for DRA to use for storing audit and cache data.
Specify DRA replication database location	<ul style="list-style-type: none"> ◆ Specify the file location for the DRA replication database and the replication service port. ◆ Specify the SSL certificate that you want to use for secure communications with the database through IIS, and specify the IIS replication port. <p>NOTE: The IIS Replication Web Site SSL Certificate field lists the certificates from both the WebHosting store and the Personal store.</p>
Specify REST Service SSL Certificate	<p>Select the SSL certificate you will use for the REST service, and specify the REST service port.</p> <p>NOTE: The REST Service SSL Certificate field lists the certificates from both the WebHosting store and Personal store.</p>
Specify Web Console SSL Certificate	Specify the SSL certificate you will use for the HTTPS binding.
Verify install configuration	You can verify the configuration on the installation summary page before clicking Install to proceed with the installation.
Post Install Verification	<p>After the installation is completed, the Health Checker will run to verify the install and update the product license.</p> <p>For more information, see “Health Check Utility” in the <i>DRA Administrator Guide</i>.</p>

Install DRA Clients

You can install specific DRA consoles and command line clients by executing the DRAInstaller.msi with the corresponding .mst package on the installation target:

NetIQDRACLI.mst	Installs the command-line interface
NetIQDRAADSI.mst	Installs the DRA ADSI provider
NetIQDRAClients.mst	Installs all DRA user interfaces

To deploy specific DRA clients to multiple computers across your enterprise, configure a group policy object to install the specific .MST package.

- 1 Start Active Directory Users and Computers and create a group policy object.
- 2 Add the DRAInstaller.msi package to this group policy object.
- 3 Ensure this group policy object has one of the following properties:
 - ◆ Each user account in the group has Power User permissions for the appropriate computer.
 - ◆ Enable the Always Install with Elevated Privileges policy setting.
- 4 Add the user interface .mst file, to this group policy object.
- 5 Distribute your group policy.

NOTE: For more information about group policy, see Microsoft Windows Help. To easily and securely test and deploy group policy across your enterprise, use *Group Policy Administrator*.

Install Workflow Automation and Configure Settings

To manage Workflow Automation requests in DRA you need to do the following:

- ◆ Install and configure Workflow Automation and the DRA Adapter.

For information see, the *Workflow Automation Administrator Guide* and the *Workflow Automation Adapter Reference for DRA*.
- ◆ Configure Workflow Automation integration with DRA.

For information, see “Configuring the Workflow Automation Server” in the *DRA Administrator Guide*.
- ◆ Delegate Workflow Automation powers in DRA.

For information, see “Delegating Workflow Automation Server Configuration Powers” in the *DRA Administrator Guide*.

The documents referenced above are available on the [DRA Documentation site](#).

Install DRA Reporting

DRA Reporting requires you to install the DRAReportingSetup.exe file from the NetIQ DRA Installation Kit.

Steps	Details
Log on to the target server	Log on to the target Microsoft Windows server for the install with an account that has local administrative privileges. Ensure this account has local and domain administrative privileges as well as System Administrator privileges on the SQL Server.

Steps	Details
Copy and run the NetIQ Admin Installation Kit	Copy the DRA installation kit NetIQAdminInstallationKit.msi to the target server and execute it by double-clicking the file or calling it from the command line. The installation kit will extract the DRA installation media to a customizable location on the local file system. In addition, the installation kit will install the .Net framework on the target server if needed to meet the requirements of the DRA product installer pre-requisite.
Execute the DRA Reporting install	Navigate to the location where the installation media was extracted and execute DRAReportingSetup.exe to install the management component for DRA reporting integration.
Verify and install prerequisites	<p>The Prerequisites page displays the list of required software based on the components selected for the installation. The installer will guide you through installing any missing prerequisites that are required for the install to complete successfully.</p> <p>For information about Reporting Center, see Reporting Center Guide on the documentation web site.</p>
Accept the EULA license agreement	Accept the terms of the End User License Agreement to finishing running the installation.

5 Product Upgrade

This chapter provides a process that helps you upgrade or migrate a distributed environment in controlled phases.

This chapter assumes your environment contains multiple Administration servers, with some servers located at remote sites. This configuration is called a Multi-Master Set (MMS). An MMS consists of one primary Administration server and one or more associated secondary Administration servers. For more information on how an MMS works, see “Configuring the Multi-Master Set” in the *DRA Administrator Guide*.

- ♦ [“Planning a DRA Upgrade” on page 47](#)
- ♦ [“Pre-Upgrade Tasks” on page 48](#)
- ♦ [“Upgrading the DRA Administration Server” on page 51](#)
- ♦ [“Upgrading Workflow Automation” on page 54](#)
- ♦ [“Upgrading Reporting” on page 55](#)

Planning a DRA Upgrade

Execute the `NetIQAdminInstallationKit.msi` to extract the DRA installation media and install and run the Health Check Utility.

Ensure you plan your deployment of DRA before you begin the upgrade process. As you plan your deployment, consider the following guidelines:

- ♦ Test the upgrade process in your lab environment before pushing the upgrade out to your production environment. Testing allows you to identify and resolve any unexpected issues without impacting daily administration responsibilities.
- ♦ Review [Required Ports and Protocols](#).
- ♦ Determine how many assistant administrators rely on each MMS. If the majority of your assistant administrators rely on specific servers or server sets, upgrade those servers first during off-peak hours.
- ♦ Determine which assistant administrators need the Delegation and Configuration console. You can obtain this information in one of the following ways:
 - ♦ Review which assistant administrators are associated with the built-in assistant administrator groups.
 - ♦ Review which assistant administrators are associated with the built-in ActiveViews.
 - ♦ Use Directory and Resource Administrator Reporting to generate security model reports, such as the ActiveView Assistant Admin Details and Assistant Admin Groups reports.

Notify these assistant administrators about your upgrade plans for the user interfaces.

- ♦ Determine which assistant administrators need to connect to the primary Administration server. These assistant administrators should upgrade their client computers once you upgrade the primary Administration server.

Notify these assistant administrators about your plans for upgrading the Administration servers and user interfaces.

- ◆ Determine whether you need to implement any delegation, configuration, or policy changes before beginning the upgrade process. Depending on your environment, this decision can be made on a site-by-site basis.
- ◆ Coordinate upgrading your client computers and your Administration servers to ensure minimal downtime. Be aware that DRA does not support running previous DRA versions with the current DRA version on the same Administration server or client computer.

Pre-Upgrade Tasks

Before you start the upgrade installations, follow the pre-upgrade steps below to prepare each server set for an upgrade.

Steps	Details
Backup the AD LDS instance	Open the Health Check Utility and run the AD LDS Instance Backup check to create a backup of your current AD LDS instance.
Make a deployment plan	Make a deployment plan for upgrading the Administration servers and user interfaces (assistant administrator client computers). For more information, see Planning a DRA Upgrade .
Dedicate a secondary server to run a previous DRA version	<i>Optional:</i> Dedicate a secondary Administration server to run a previous DRA version as you upgrade a site.
Make required changes for this MMS	Make any necessary changes to the delegation, configuration, or policy settings for this MMS. Use the primary Administration server to modify these settings.
Synchronize the MMS	Synchronize the server sets so each Administration server contains the latest configuration and security settings.
Back up the primary server registry	Back up the registry from the primary Administration server. Having a backup of your previous registry settings allows you to easily recover your previous configuration and security settings.
Convert gMSA to DRA user accounts	<i>Optional:</i> If you are using a group Managed Service Account (gMSA) for the DRA Service account, change the gMSA account to a DRA user account before you upgrade. Post-upgrade, you will need to change the account back to a gMSA.

NOTE: If you need to restore the AD LDS Instance, do the following:

- 1 Stop the current AD LDS Instance in Computer Management > Services. This will have a different title: NetIQDRASecureStoragexxxxx.
 - 2 Replace the **current** adamnts.dit file with the **backup** adamnts.dit file as indicated below:
 - ◆ Current file location: %ProgramData%/NetIQ/DRA/<DRAInstanceName>/data/
 - ◆ Backup file location: %ProgramData%/NetIQ/ADLDS/
 - 3 Restart the AD LDS instance.
-

Pre-upgrade topics:

- ♦ [“Dedicating a Local Administration Server to Run a Previous DRA Version” on page 49](#)
- ♦ [“Synchronizing Your Previous DRA Version Server Set” on page 50](#)
- ♦ [“Backing Up the Administration Server Registry” on page 50](#)

Dedicating a Local Administration Server to Run a Previous DRA Version

Dedicating one or more secondary Administration servers to run a previous DRA version locally at a site during an upgrade can help minimize downtime and costly connections to remote sites. This step is optional and allows assistant administrators to use a previous DRA version throughout the upgrade process, until you are satisfied that your deployment is complete.

Consider this option if you have one or more of the following upgrade requirements:

- ♦ You require little or no downtime.
- ♦ You must support a large number of assistant administrators, and you are not able to upgrade all client computers immediately.
- ♦ You want to continue supporting access to a previous DRA version after you upgrade the primary Administration server.
- ♦ Your environment includes an MMS that spans across multiple sites.

You can install a new secondary Administration server or designate an existing secondary server running a previous DRA version. If you intend to upgrade this server, this server should be the last server you upgrade. Otherwise, completely uninstall DRA from this server when you successfully finish your upgrade.

Setting Up a New Secondary Server

Installing a new secondary Administration server at a local site can help you avoid costly connections to remote sites, and ensures your assistant administrators can continue using a previous DRA version without interruption. If your environment includes an MMS that spans across multiple sites, you should consider this option. For example, if your MMS consists of a primary Administration server at your London site and a secondary Administration server at your Tokyo site, consider installing a secondary server at the London site and adding it to the corresponding MMS. This additional server allows assistant administrators from the London site to use a previous DRA version until the upgrade is complete.

Using an Existing Secondary Server

You can use an existing secondary Administration server as the dedicated server for a previous DRA version. If you do not plan to upgrade a secondary Administration server at a given site, you should consider this option. If you cannot dedicate an existing secondary server, consider installing a new Administration server for this purpose. Dedicating one or more secondary servers to run a previous DRA version allows your assistant administrators to continue using a previous DRA version without interruption until the upgrade is complete. This option works best in larger environments that use a centralized administration model.

Synchronizing Your Previous DRA Version Server Set

Before you back up the previous DRA version registry or begin the upgrade process, ensure you synchronize the server sets so each Administration server contains the latest configuration and security settings.

NOTE: Ensure you made all necessary changes to the delegation, configuration, or policy settings for this MMS. Use the primary Administration server to modify these settings. Once you upgrade the primary Administration server, you cannot synchronize delegation, configuration, or policy settings to any Administration servers running previous DRA versions.

To synchronize your existing server set:

- 1 Log in to the primary Administration server as the Built-in Admin.
- 2 Open the Delegation and Configuration Console and expand **Configuration Management**.
- 3 Click **Administration servers**.
- 4 In the right pane, select the appropriate primary Administration server for this server set.
- 5 Click **Properties**.
- 6 On the Synchronization schedule tab, click **Refresh Now**.
- 7 Verify the successful completion of the synchronization, and that all secondary Administration servers are available.

Backing Up the Administration Server Registry

Backing up the Administration server registry ensures that you can return to your previous configurations. For example, if you must completely uninstall the current DRA version and use the previous DRA version, having a backup of your previous registry settings allows you to easily recover your previous configuration and security settings.

However, be careful when editing your registry. If there is an error in your registry, the Administration server may not function as expected. If an error occurs during the upgrade process, you can use the backup of your registry settings to restore the registry. For more information, see the *Registry Editor Help*.

IMPORTANT

- ♦ The DRA server version, Windows OS name and managed domain configuration must be the same when restoring the registry.
 - ♦ Before upgrading, back up the Windows OS of the machine that is hosting DRA or create a virtual machine snapshot image of the machine.
-

To back up the Administration Server registry:

- 1 Run `regedit.exe`.
- 2 Right-click the `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Mission Critical Software\OnePoint` node, and select **Export**.
- 3 Specify the name and location of the file to save the registry key, and click **Save**.

Upgrading the DRA Administration Server

The following checklist guides you through the entire upgrade process. Use this process to upgrade each server set in your environment. If you have not done it yet, use the Health Check Utility to create a backup of your current AD LDS instance.

WARNING: Do not upgrade your secondary Administration servers until you have upgraded the primary Administration server for that MMS.

You can spread the upgrade process over several phases, upgrading one MMS at a time. This upgrade process also allows you to temporarily include secondary servers running a previous DRA version and secondary servers running the current DRA version in the same MMS. DRA supports synchronization between Administration servers running a previous DRA version and servers running the current DRA version. However, be aware that DRA does not support running a previous DRA version with the current DRA version on the same Administration server or client computer.

IMPORTANT: For the successful replication of temporary group assignments in the secondary server, run the **Multi-master synchronization schedule** manually or wait for its scheduled run.

Steps	Details
Run Health Check utility	Install the standalone DRA Health Check utility and run it using a service account. Fix any issues.
Perform a test upgrade	Perform a test upgrade in your lab environment to identify potential issues and minimize production downtime.
Determine the order of upgrade	Determine the order in which you want to upgrade your server sets.
Prepare each MMS for upgrade	Prepare each MMS for an upgrade. For more information, see Pre-Upgrade Tasks .
Upgrade primary server	Upgrade the primary Administration server in the appropriate MMS. For information, see Upgrading the Primary Administration Server .
Install new secondary server	<i>(Optional)</i> To minimize downtime at remote sites, install a local secondary Administration server running the newest version of DRA. For information, see Installing a Local Secondary Administration Server for the Current DRA Version .
Deploy user interfaces	Deploy the user interfaces to your assistant administrators. For information, see Deploying the DRA User Interfaces
Upgrade secondary servers	Upgrade the secondary Administration servers in the MMS. For information, see Upgrading Secondary Administration Servers .
Upgrade DRA Reporting	Upgrade DRA Reporting. For information, see Upgrading Reporting .
Run Health Check utility	Run the Health Check Utility that was installed as part of the upgrade. Fix any issues.

Steps	Details
Update Web Console configuration (post-upgrade)	<p>(Conditional, post-upgrade) If you have either of the Web Console configurations below before an upgrade, they will need to be updated after the upgrade installation completes:</p> <ul style="list-style-type: none">◆ Default server connections enabled◆ Modified configuration files <p>For more information, see Updating the Web Console Configuration - Post Installation.</p>

Server upgrade topics:

- ◆ [“Upgrading the Primary Administration Server” on page 52](#)
- ◆ [“Installing a Local Secondary Administration Server for the Current DRA Version” on page 52](#)
- ◆ [“Deploying the DRA User Interfaces” on page 53](#)
- ◆ [“Upgrading Secondary Administration Servers” on page 53](#)
- ◆ [“Updating the Web Console Configuration - Post Installation” on page 54](#)

Upgrading the Primary Administration Server

Before you upgrade, notify your assistant administrators when you plan to start this process. If you dedicated a secondary Administration server to run a previous DRA version, also identify this server so assistant administrators can continue using the previous DRA version during the upgrade.

After you successfully prepare your MMS, upgrade the primary Administration server. Do not upgrade user interfaces on the client computers until you complete upgrading the primary Administration server. For more information, see [Deploying the DRA User Interfaces](#).

For more upgrade considerations and instructions, see the *Directory and Resource Administrator Release Notes*.

NOTE: Once you upgrade the primary Administration server, you cannot synchronize delegation, configuration, or policy settings from this server to secondary Administration servers running a previous DRA version.

Installing a Local Secondary Administration Server for the Current DRA Version

Installing a new secondary Administration server to run the current DRA version at a local site can help you minimize costly connections to remote sites while decreasing overall downtime and allowing quicker deployment of the user interfaces. This step is optional and allows assistant administrators to use both the current DRA version and a previous DRA version throughout the upgrade process, until you are satisfied that your deployment is complete.

Consider this option if you have one or more of the following upgrade requirements:

- ◆ You require little or no downtime.

- ◆ You must support a large number of assistant administrators, and you are not able to upgrade all client computers immediately.
- ◆ You want to continue supporting access to a previous DRA version after you upgrade the primary Administration server.
- ◆ Your environment includes an MMS that spans across multiple sites.

For example, if your MMS consists of a primary Administration server at your London site and a secondary Administration server at your Tokyo site, consider installing a secondary server at the Tokyo site and adding it to the corresponding MMS. This additional server better balances the daily administration load at the Tokyo site, and allows assistant administrators from either site to use a previous DRA version as well as the current DRA version until the upgrade is complete. Additionally, your assistant administrators experience no downtime because you can immediately deploy the current DRA user interfaces. For more information about upgrading user interfaces, see [Deploying the DRA User Interfaces](#).

Deploying the DRA User Interfaces

Typically, you should deploy the current DRA user interfaces after you upgrade the primary Administration server and one secondary Administration server. However, for assistant administrators who must use the primary Administration server, ensure you upgrade their client computers first by installing the Delegation and Configuration console. For more information, see [Planning a DRA Upgrade](#).

If you often perform batch processing through the CLI, the ADSI provider, PowerShell, or frequently generate reports, consider installing these user interfaces on a dedicated secondary Administration server to maintain an appropriate load balance across the MMS.

You can let your assistant administrators install the DRA user interfaces or deploy these interfaces through group policy. You can also easily and quickly deploy the Web Console to multiple assistant administrators.

NOTE: You cannot run multiple versions of DRA components side-by-side on the same DRA server. If you plan to gradually upgrade your assistant administrator client computers, consider deploying the Web Console to ensure immediate access to an Administration server running the current DRA version.

Upgrading Secondary Administration Servers

When upgrading secondary Administration servers, you can upgrade each server as needed, depending on your administration requirements. Also, consider how you plan to upgrade and deploy the DRA user interfaces. For more information, see [Deploying the DRA User Interfaces](#).

For example, a typical upgrade path may include the following steps:

- 1 Upgrade one secondary Administration server.
- 2 Instruct the assistant administrators who use this server to install the appropriate user interfaces, such as the Web Console.
- 3 Repeat steps 1 and 2 above until you completely upgrade the MMS.

Before you upgrade, notify your assistant administrators when you plan to start this process. If you dedicated a secondary Administration server to run a previous DRA version, also identify this server so assistant administrators can continue using the previous DRA version during the upgrade. When you complete the upgrade process for this MMS, and all assistant administrator client computers are running upgraded user interfaces, take any remaining previous DRA version servers offline.

Updating the Web Console Configuration - Post Installation

Perform either or both of the actions below, post-upgrade installation, if they apply to your DRA environment:

Default DRA Server Connection

The DRA REST Service component is consolidated with the DRA Server beginning in DRA 10.1. If you have the default DRA Server connection configured before you upgrade from a DRA 10.0.x or earlier version, you need to review those settings post-upgrade as there is now only one connection configuration, the DRA Server Connection. You can access this configuration in the Web Console at **Administration > Configuration > DRA Server Connection**.

You can also update these settings post-upgrade in the `web.config` file at `C:\inetpub\wwwroot\DRAClient\rest` on the DRA Web Console server, as follows:

```
<restService useDefault="Never">  
<serviceLocation address="<REST server name>" port="8755"/>  
</restService>
```

Web Console Login Configuration

When upgrading from DRA 10.0.x or earlier versions, if the DRA REST Service is installed without the DRA Server, uninstalling the DRA REST Service is a prerequisite for an upgrade. A copy of files that were modified before the upgrade is made to `C:\ProgramData\NetIQ\DRA\Backup\` on the server. You can use these files for reference to update any relevant ones after the upgrade.

Upgrading Workflow Automation

To perform an in-place upgrade on non-clustered 64-bit environments, simply run the Workflow Automation setup program on your existing Workflow Automation computers. It is not necessary to stop any Workflow Automation services that may be running.

Note: Any Workflow Automation adapters that are not built-in to the Workflow Automation installer must be uninstalled and reinstalled post-upgrade.

For more detailed information about upgrading Workflow Automation, see “Upgrading from a Previous Version” in the [Workflow Automation Administrator Guide](#).

Upgrading Reporting

Before you upgrade DRA Reporting, ensure that your environment meets the minimum requirements for NRC 3.3.2 For more information on installation requirements and upgrade considerations, see the *Reporting Center Reporting Guide*.

Steps	Details
Disable DRA Reporting Support	To ensure that the reporting collectors do not run during the upgrade process, disable DRA reporting support on the Reporting Service Configuration window in the Delegation and Configuration console.
Log on to the SQL instance server with applicable credentials	Log on to the Microsoft Windows server where you have installed the SQL instance for the reporting databases with an administrator account. Ensure this account has local administrative privileges as well as System Administrator privileges on the SQL Server.
Run the DRA Reporting setup	Run <code>DRAReportingSetup.exe</code> from the installation kit and follow the instructions in the installation wizard.
Enable DRA Reporting Support	On your primary administration server, enable reporting in the Delegation and Configuration Console.

If your environment uses SSRS integration, you will need to re-deploy your reports. For more information about re-deploying reports, see [Reporting Center Guide](#) on the documentation web site.



Delegation Model

DRA enables administrators to implement a “least privilege” permissions scheme by providing a flexible set of controls for granting granular powers to specific managed objects in the enterprise. Through these delegations, administrators can ensure that assistant administrators receive just the permissions needed to complete their specific roles and responsibilities.

- ♦ [Chapter 6, “Understanding the Dynamic Delegation Model,” on page 59](#)
- ♦ [Chapter 7, “ActiveViews,” on page 65](#)
- ♦ [Chapter 8, “Roles,” on page 69](#)
- ♦ [Chapter 9, “Powers,” on page 79](#)
- ♦ [Chapter 10, “Delegation Assignments,” on page 83](#)

6 Understanding the Dynamic Delegation Model

DRA enables you to manage administrative access to your enterprise within the context of a delegation model. The delegation model allows you to set up “least privilege” access for assistant administrators through a dynamic set of controls that can adapt as the enterprise changes and evolves. The delegation model provides administrative access control that more closely represents how your company works by:

- ◆ With flexible scoping rules, administrators can target permissions to specific managed objects based on business needs instead of the structure of the enterprise.
- ◆ Roles based delegation ensures that permissions are consistently granted and simplifies provisioning.
- ◆ Privilege assignment can be administered across domains, cloud tenants, and managed applications from a single location.
- ◆ Granular powers enable you to tailor the specific access granted to assistant administrators.

Delegation Model Controls

Administrators use the following controls to provision access through the delegation model:

- ◆ **Delegation:** Administrators provision access to users and groups by assigning a role, which has specified permissions in the context of an ActiveView that provides the scope.
- ◆ **ActiveViews:** An ActiveView represents a specific scope of managed objects which are defined by one or more rules. Managed objects identified by each rule in an ActiveView are aggregated together into a unified scope.
- ◆ **ActiveView Rule:** Rules are defined by expressions that match a set of managed objects based on a number of conditions such as object type, location, name, and so forth.
- ◆ **Roles:** A role represents a specific set of powers (permissions) required to perform a specific administration function. DRA provides a number of built-in roles for common business functions, and you can define custom roles that best fit your organization’s needs.
- ◆ **Powers:** A power defines a specific permission for tasks supported by the managed object such as view, modify, create, delete, and so forth. Permissions around the modification of a managed object can be further broken down to the specific properties that can be changed. DRA provides an extensive list of built-in powers for supported managed objects and can define custom powers to extend what can be provisioned through the delegation model.

How DRA Processes Requests

When the Administration server receives a request for an action, such as changing a user password, it uses the following process:

1. Search for ActiveViews that are configured to manage the target object of the operation.
2. Validate the powers assigned to the account that is requesting the action.
 - a. Evaluate all Active View assignments that contain the assistant administrator requesting the operation.
 - b. Once that list is complete, build a list of all ActiveViews that contain both the target object and the assistant administrator.
 - c. Compare the powers to the powers needed for the requesting operation.
3. *If the account has the correct power*, the Administration server allows the action to be performed.
If the account does not have the correct power, the Administration server returns an error.
4. Update Active Directory.

Examples of How DRA Processes Delegation Assignments

The following examples describe common scenarios that arise in how DRA evaluates the delegation model when processing a request:

Example 1: Changing a User's Password

When an assistant administrator attempts to set a new password for the JSmith user account, the Administration server finds all ActiveViews that include JSmith. This search looks for any ActiveView that specifies JSmith directly, through a wildcard rule or group membership. If an ActiveView includes other ActiveViews, the Administration server also searches these additional ActiveViews. The Administration server determines whether the assistant administrator has the *Reset User Account Password* power in any of these ActiveViews. If the assistant administrator has the *Reset User Account Password* power, the Administration server resets the password for JSmith. If he does not have this power, the Administration server denies the request.

Example 2: Overlapping ActiveViews

A power defines the properties of an object an assistant administrator can view, modify, or create in your managed domain or subtree. More than one ActiveView can include the same object. This configuration is called **overlapping ActiveViews**.

When ActiveViews overlap, you can accumulate a set of different powers over the same objects. For example, if one ActiveView allows you to add a user account to a domain and another ActiveView allows you to delete a user account from the same domain, you can add or delete user accounts in that domain. In this way, the powers you have over a given object are cumulative.

It is important to understand how ActiveViews can overlap and you can have increased powers over objects included in these ActiveViews. Consider the ActiveView configuration illustrated in the following figure.



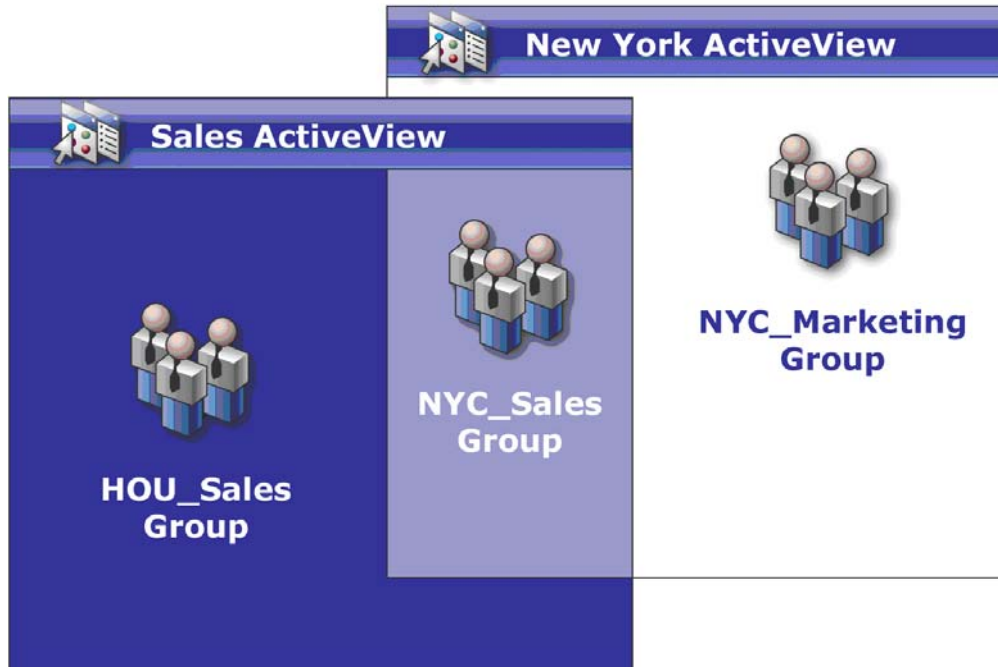
The white tabs identify ActiveViews by location, *New York City* and *Houston*. The black tabs identify ActiveViews by their organizational function, *Sales* and *Marketing*. The cells show the groups included in each ActiveView.

The NYC_Sales group and the HOU_Sales group are both represented in the Sales ActiveView. If you have power in the Sales ActiveView, then you can manage any member of the NYC_Sales and HOU_Sales groups. If you also have power in the New York City ActiveView, then these additional powers apply to the NYC_Marketing group. In this way, powers accumulate as the ActiveViews overlap.

Overlapping ActiveViews can provide a powerful, flexible delegation model. However, this feature can also have unintended consequences. Carefully plan your ActiveViews to ensure each assistant administrator has only the powers you intend over each user account, group, OU, contact, or resource.

Groups in Multiple ActiveViews

In this example, the NYC_Sales group is represented in more than one ActiveView. The members of the NYC_Sales group are represented in the New York City ActiveView because the group name matches the NYC_* ActiveView rule. The group is also in the Sales ActiveView because the group name matches the *_Sales ActiveView rule. By including the same group in multiple ActiveViews, you can allow different assistant administrators to manage the same objects differently.



Using Powers in Multiple ActiveViews

Assume there is an assistant administrator, JSmith, who has the *Modify General User Properties* power in the New York City ActiveView. This first power allows JSmith to edit all the properties on the General tab of a user properties window. JSmith has the *Modify User Profile Properties* power in the Sales ActiveView. This second power allows JSmith to edit all the properties on the Profile tab of a user properties window.

The following figure indicates the powers JSmith has for each group.

	Sales ActiveView (*_Sales)	Marketing ActiveView (*_Marketing)
New York City ActiveView (NYC_*)	 <p>!General Properties !Profile Properties NYC_Sales Group</p>	 <p>!General Properties NYC_Marketing Group</p>
Houston ActiveView (HOU_*)	 <p>!Profile Properties HOU_Sales Group</p>	 <p>!No Powers HOU_Marketing Group</p>

JSmith has the following powers:

- ◆ General Properties in the NYC_* ActiveView
- ◆ Profile Properties in the *_Sales ActiveView

The power delegation in these overlapping ActiveViews allows JSmith to modify the General and Profile properties of the NYC_Sales group. Thus, JSmith has all the powers granted in all the ActiveViews that represent the NYC_Sales group.

7 ActiveViews

ActiveViews enable you to implement a delegation model that has the following features:

- ♦ Is independent of your Active Directory structure
- ♦ Allows you to assign powers and define policies that correlate to your existing workflows
- ♦ Provides automation to help you further integrate and customize your enterprise
- ♦ Dynamically responds to change

An ActiveView represents a set of objects within one or more managed domains. You can include an object in more than one ActiveView. You can also include many objects from multiple domains or OUs.

Built-in ActiveViews

Built-in ActiveViews are the default ActiveViews provided by DRA. These ActiveViews represent all current objects and security settings. Thus, built-in ActiveViews provide immediate access to all your objects and settings as well as the default delegation model. You can use these ActiveViews to manage objects, such as user accounts and resources, or apply the default delegation model to your current enterprise configuration.

DRA provides several built-in ActiveViews that can represent your delegation model. The built-in ActiveView node contains the following ActiveViews:

All Objects

Includes all objects in all managed domains. Through this ActiveView, you can manage any aspect of your enterprise. Assign this ActiveView to the administrator or to an assistant administrator who needs auditing powers across the enterprise.

Objects Current User Manages as Windows Administrator

Includes objects from the current managed domain. Through this ActiveView, you can manage user accounts, groups, contacts, OUs, and resources. Assign this ActiveView to native administrators who are responsible for account and resource objects in the managed domain.

Administration Servers and Managed Domains

Includes Administration server computers and managed domains. Through this ActiveView, you can manage the daily maintenance of your Administration servers. Assign this ActiveView to assistant administrators whose duties include monitoring the synchronization status or performing cache refreshes.

DRA Policies and Automation Triggers

Includes all policy and automation trigger objects in all managed domains. Through this ActiveView, you can manage policy properties and scope, as well as automation trigger properties. Assign this ActiveView to assistant administrators responsible for creating and maintaining your company policies.

DRA Security Objects

Includes all security objects. Through this ActiveView, you can manage ActiveViews, assistant administrator groups, and roles. Assign this ActiveView to assistant administrators responsible for creating and maintaining your security model.

SPA Users from All Managed and Trusted Domains

Includes all user accounts from managed and trusted domains. Through this ActiveView, you can manage user passwords via Secure Password Administrator (SPA).

Accessing Built-in ActiveViews

Access built-in ActiveViews to audit the default delegation model or manage your own security settings.

To access built-in ActiveViews:

- 1 Navigate to **Delegation Management > Manage ActiveViews**.
- 2 Ensure the search field is blank, and click **Find Now** in the **List items that match my criteria** pane.
- 3 Select the appropriate ActiveView.

Using Built-in ActiveViews

You cannot delete, clone, or modify built-in ActiveViews. However, you can incorporate these ActiveViews into your existing delegation model or use these ActiveViews to design your own model.

You can use built-in ActiveViews in the following ways:

- ◆ Assign the individual built-in ActiveViews to the appropriate assistant administrator groups. This association allows the assistant administrator group members to manage the corresponding set of objects with the appropriate powers.
- ◆ Refer to the built-in ActiveView rules and associations as guidelines for designing and implementing your delegation model.

For more information about designing a dynamic delegation model, see [Understanding the Dynamic Delegation Model](#).

Implementing a Custom ActiveView

An ActiveView provides real-time access to specific objects within one or more domains or OUs. You can add or remove objects from an ActiveView without changing the underlying domain or OU structure.

You may think of an ActiveView as a virtual domain or OU, or the results of a select statement or database view for a relational database. ActiveViews can include or exclude any set of objects, contain other ActiveViews, and have overlapping contents. ActiveViews can contain objects from different domains, trees, and forests. You can configure ActiveViews to meet any enterprise management need.

ActiveViews can include the following object types:

Accounts:

- ◆ Users
- ◆ Groups
- ◆ Computers
- ◆ Contacts
- ◆ Dynamic Distribution Groups
- ◆ Group Managed Service Account
- ◆ Published Printers
- ◆ Published Printer Print Jobs
- ◆ Resource Mailboxes
- ◆ Shared Mailboxes
- ◆ Public Folders
- ◆ Remote User Mailboxes
- ◆ Remote Shared Mailboxes

Directory Objects:

- ◆ Organizational Units
- ◆ Domains
- ◆ Member Servers

Delegation Objects:

- ◆ ActiveViews
- ◆ Self Administration
- ◆ Direct Reports
- ◆ Managed Groups

Resources:

- ◆ Connected Users
- ◆ Devices
- ◆ Event Logs
- ◆ Open Files
- ◆ Printers
- ◆ Print Jobs
- ◆ Services
- ◆ Shares

Azure Objects:

- ◆ Azure User
- ◆ Azure Guest User
- ◆ Azure Group

- ◆ Azure Tenant
- ◆ Azure Contact

As your enterprise changes or grows, ActiveViews change to include or exclude the new objects. Thus, you can use ActiveViews to reduce the complexity of your model, provide the security you need, and give you far more flexibility than other enterprise organizing tools.

ActiveViews Rules

An ActiveView can consist of rules that include or exclude objects such as user accounts, groups, OUs, contacts, resources, computers, resource mailboxes, shared mailboxes, dynamic distribution groups, group Managed Service Accounts, ActiveViews, and Azure objects such as Azure users, Azure guest users, Azure groups, and Azure contacts. This flexibility makes ActiveViews dynamic.

These matches are called **wildcards**. For example, you can define a rule to include all computers with names matching `DOM*`. This wildcard specification will search for any computer account whose name begins with the character string `DOM`. Wildcard matching makes administration dynamic because accounts are automatically included when they match the rule. Thus, when you use wildcards, you do not need to reconfigure the ActiveViews as your organization changes.

Another example is defining ActiveViews based on group membership. You can define a rule that includes all members of groups that begin with the letters `NYC`. Then, as members are added to any group matching this rule, these members are automatically included in this ActiveView. As your enterprise changes or grows, DRA reapplies the rules to include or exclude the new objects in the proper ActiveViews.

8 Roles

This section includes a list with descriptions of the roles that are built-in into DRA, how to use those roles, and information about creating and managing custom roles.

For a description of roles and their use in general, see [Delegation Model Controls](#).

Built-in Roles

Built-in assistant administrator roles provide immediate access to a set of commonly used powers. You can extend your current security configuration by using these default roles to delegate power to specific user accounts or other groups.

These roles contain the powers required to perform common administration tasks. For example, the DRA Administration role contains all the powers required to manage objects. To use these powers, however, the role must be associated with a user account or an assistant administrator group and the managed ActiveView.

Because built-in roles are part of the default delegation model, you can use the built-in roles to quickly delegate power and implement security. These built-in roles address common tasks you can perform through the DRA user interfaces. The following sections describe each built-in role and summarize the powers associated with that role.

Azure Active Directory Management

Azure Contact Administration

Provides all the powers required to create, modify, delete, and view properties of an Azure contact. You can assign this role to all assistant administrators who are responsible for managing Azure contacts.

Azure Group Administration

Provides all the powers required to manage Azure groups and Azure membership.

Azure User Administration

Provides all the powers required to create, modify, delete, enable, disable, and view properties of an Azure user. Assign this role to assistant administrators responsible for managing Azure users.

Azure Guest User Administration

Provides all the powers required to manage an Azure guest user. Assign this role to assistant administrators responsible for managing an Azure guest user.

Administration

Contact Administration

Provides all the powers required to create a new contact, modify contact properties, or delete a contact. Assign this role to assistant administrators responsible for managing contacts.

DRA Administration

Provides all powers to an assistant administrator. This role gives a user the permission to perform all administration tasks within DRA. This role is equivalent to the permissions of an administrator. An assistant administrator associated with the DRA Administration role can access all Directory and Resource Administrator nodes.

gMSA Administration

Provides the powers required to create, modify, delete, and view properties of a group Managed Service Account (gMSA). You can assign this role to all assistant administrators who are responsible for managing a gMSA.

Manage and Execute Custom Tools

Provides all the powers required to create, manage, and execute custom tools. Assign this role to assistant administrators responsible for managing custom tools.

Manage Clone Exceptions

Provides all the powers required to create and manage clone exceptions.

Manage Policies and Automation Triggers

Provides all the powers required to define policies and automation triggers. Assign this role to assistant administrators responsible for maintaining company policies and automating workflows.

Manage Security Model

Provides all the powers required to define the Administration rules, including ActiveViews, assistant administrators, and roles. Assign this role to assistant administrators responsible for implementing and maintaining your security model.

Manage Virtual Attributes

Provides all the powers required to create and manage virtual attributes. Assign this role to assistant administrators responsible for managing virtual attributes.

OU Administration

Provides all the powers required to manage organizational units. Assign this role to assistant administrators responsible for managing the Active Directory structure.

Public Folder Administration

Provides the powers to create, modify, delete, enable, or disable mail and view the properties of your Public Folder. You can assign this role to all assistant administrators who are responsible for managing Public Folder.

Replicate Files

Provides all the powers required to upload, delete, and modify file information. Assign this role to assistant administrators responsible for replicating files from the primary Administration server to other Administration servers in the MMS and the DRA client computers.

Reset Local Administrator Password

Provides all the powers to reset the local administrator account password and view the name of the computer administrator. Assign this role to assistant administrators responsible for managing the administrator accounts.

Self Administration

Provides all the powers required to modify basic properties, such as telephone numbers, of your own user account. Assign this role to assistant administrators to allow them to manage their own personal information.

Advanced Query Management

Execute Advanced Queries

Provides all the powers required to execute saved advanced queries. Assign this role to assistant administrators responsible for executing advanced queries.

Manage Advanced Queries

Provides all the powers required to create, manage, and execute advanced queries. Assign this role to assistant administrators responsible for managing advanced queries.

Audit Management

Audit All Objects

Provides all the powers required to view properties of objects, policies, and configurations across your enterprise. This role does not allow an assistant administrator to modify properties. Assign this role to assistant administrators responsible for auditing actions across your enterprise. Allows assistant administrators to view all nodes except the Custom Tools node.

Audit Limited Account and Resource Properties

Provides powers for all object properties.

Audit Resources

Provides all the powers required to view properties of managed resources. Assign this role to assistant administrators responsible for auditing resource objects.

Audit Users and Groups

Provides all the powers needed to view user account and group properties, but no powers to modify these properties. Assign this role to assistant administrators responsible for auditing account properties.

Computer Management

Computer Administration

Provides all the powers required to modify computer properties. This role allows assistant administrators to add, delete, and shut down computers, as well as synchronize domain controllers. Assign this role to assistant administrators responsible for managing computers in the ActiveView.

Create and Delete Computer Accounts

Provides all the powers required to create and delete a computer account. Assign this role to assistant administrators responsible for managing computers.

Manage Computer Properties

Provides all the powers required to manage all properties for a computer account. Assign this role to assistant administrators responsible for managing computers.

View All Computer Properties

Provides all the powers required to view properties of a computer account. Assign this role to assistant administrators responsible for auditing computers.

Exchange Management

Clone User with Mailbox

Provides all the powers required to clone an existing user account along with the account mailbox. Assign this role to assistant administrators responsible for managing user accounts.

NOTE: To allow the assistant administrator to add the new user account to a group during the clone task, also assign the Manage Group Memberships role.

Create and Delete Resource Mailbox

Provides all the powers required to create and delete a mailbox. Assign this role to assistant administrators responsible for managing mailboxes.

Mailbox Administration

Provides all the powers required to manage Microsoft Exchange mailbox properties. If you use Microsoft Exchange, assign this role to assistant administrators responsible for managing Microsoft Exchange mailboxes.

Manage Exchange Mailbox Rights

Provides all the powers required to manage security and rights for Microsoft Exchange mailboxes. If you use Microsoft Exchange, assign this role to assistant administrators responsible for managing Microsoft Exchange mailbox permissions.

Manage Group Email

Provides all the powers required to view, enable, or disable the email address for a group. Assign this role to assistant administrators responsible for managing groups or email addresses for account objects.

Manage Mailbox Move Requests

Provides all the powers required to manage mailbox move requests.

Manage Resource Mailbox Properties

Provides all the powers required to manage all properties for a mailbox. Assign this role to assistant administrators responsible for managing mailboxes.

Manage User Email

Provides all the powers required to view, enable, or disable the email address for a user account. Assign this role to assistant administrators responsible for managing user accounts or email addresses for account objects.

Reset Unified Messaging PIN Properties

Provides all the powers required to reset Unified Messaging PIN properties for user accounts.

Resource Mailbox Administration

Provides all the powers required to manage resource mailboxes.

Shared Mailbox Administration

Provides all the powers required to create, modify, delete, and view the properties of your shared mailboxes. Assign this role to all assistant administrators responsible for managing shared mailboxes.

View All Resource Mailbox Properties

Provides all the powers required to view properties for a resource mailbox. Assign this role to assistant administrators responsible for auditing resource mailboxes.

Group Management

Create and Delete Groups

Provides all the powers required to create and delete a group. Assign this role to assistant administrators responsible for managing groups.

Dynamic Group Administration

Provides all the powers required to manage Active Directory dynamic groups.

Group Administration

Provides all the powers required to manage groups and group memberships, and view corresponding user properties. Assign this role to assistant administrators responsible for managing groups or account and resource objects that are managed through groups.

Manage Dynamic Distribution Groups

Provides all the powers required to manage Microsoft Exchange dynamic distribution groups.

Manage Group Membership Security

Provides all the powers required to designate who can view and modify Microsoft Windows group memberships through Microsoft Outlook

Manage Group Memberships

Provides all the powers required to add and remove user accounts or groups from an existing group, and view the primary group of a user or computer account. Assign this role to assistant administrators responsible for managing groups or user accounts.

Manage Group Properties

Provides all the powers required to manage all properties for a group. Assign this role to assistant administrators responsible for managing groups.

Manage Temporary Group Assignments

Provides all the powers required to create and manage temporary group assignments. Assign this role to assistant administrators responsible for managing groups.

Rename Group and Modify Description

Provides all the powers required to modify the name and description of a group. Assign this role to assistant administrators responsible for managing groups.

View All Group Properties

Provides all the powers required to view properties for a group. Assign this role to assistant administrators responsible for auditing groups.

Reporting Management

Manage Active Directory Collectors, DRA Collectors, and Management Reporting Collectors

Provides all the powers required to manage Active Directory Collectors, DRA Collectors, and Management Reporting Collectors for data collection. Assign this role to assistant administrators responsible for managing reporting configuration.

Manage Active Directory Collectors, DRA Collectors, Management Reporting Collectors, and Database Configuration

Provides all the powers required to manage Active Directory Collectors, DRA Collectors, Management Reporting Collectors, and database configuration for data collection. Assign this role to assistant administrators responsible for managing reporting and database configuration.

Manage UI Reporting

Provides all the powers required to generate and export Activity Detail reports for users, groups, contacts, computers, organizational units, powers, roles, ActiveViews, containers, published printers, and assistant administrators. Assign this role to assistant administrators responsible for generating reports.

Manage Database Configuration

Provides all the powers required to manage database configuration for Management reports. Assign this role to assistant administrators responsible for managing reporting database configuration.

View Active Directory Collectors, DRA Collectors, Management Reporting Collectors, and Database Configuration Information

Provides all the powers required to view AD collectors, DRA collectors, management reporting collectors, and database configuration information.

Resource Management

Create and Delete Resources

Provides all the powers required to create and delete shares and computer accounts, and clear event logs. Assign this role to assistant administrators responsible for managing resource objects and event logs.

Manage Printers and Print Jobs

Provides all the powers required to manage printers, print queues, and print jobs. To manage print jobs associated with a user account, the print job and the user account must be included in the same ActiveView. Assign this role to assistant administrators responsible for maintaining printers and managing print jobs.

Manage Resources for Managed Users

Provides all the powers required to manage resources associated with specific user accounts. The assistant administrator and the user accounts must be included in the same ActiveView. Assign this role to assistant administrators responsible for managing resource objects.

Manage Services

Provides all the powers required to manage services. Assign this role to assistant administrators responsible for managing services.

Manage Shared Folders

Provides all the powers required to manage shared folders. Assign this role to assistant administrators responsible for managing shared folders.

Resource Administration

Provides all the powers required to modify properties of managed resources, including resources associated with any user account. Assign this role to assistant administrators responsible for managing resource objects.

Start and Stop Resources

Provides all the powers required to pause, start, resume, or stop a service, start or stop a device or printer, shut down a computer, or synchronize your domain controllers. Also provides all the powers required to pause, resume, and start services, stop devices or print queues, and shut down computers. Assign this role to assistant administrators responsible for managing resource objects.

Server Management

Built-in Scheduler - Internal Use Only

Provides powers to schedule when DRA refreshes the cache.

Application Servers Administration

Provides the powers required to configure, view, and delete application server configurations.

Configure Servers and Domains

Provides all the powers required to modify Administration server options and managed domains. Also provides powers necessary to configure and manage Azure tenants. Assign this role to assistant administrators responsible for monitoring and maintaining the Administration servers and managing Azure tenants.

Unified Change History Server Administration

Provides the powers required to configure, view, and delete Unified Change History server configurations.

Workflow Automation Server Administration

Provides the powers required to configure, view, and delete Workflow Automation server configurations.

User Account Management

Create and Delete User Accounts

Provides all the powers required to create and delete a user account. Assign this role to assistant administrators responsible for managing user accounts.

Help Desk Administration

Provides all the powers required to view user account properties, and to change passwords and password-related properties. This role also allows assistant administrators to disable, enable, and unlock user accounts. Assign this role to assistant administrators responsible for Help Desk duties associated with ensuring users have proper access to their accounts.

Manage User Dial in Properties

Provides all the powers required to modify the dial in properties of user accounts. Assign this role to assistant administrators responsible for managing user accounts that have remote access to the enterprise.

Manage User Password and Unlock Account

Provides all the powers required to reset the password, specify password settings, and unlock a user account. Assign this role to assistant administrators responsible for maintaining user account access.

Manage User Properties

Provides all the powers required to manage all properties for a user account, including Microsoft Exchange mailbox properties. Assign this role to assistant administrators responsible for managing user accounts.

Rename User and Modify Description

Provides all the powers required to modify the name and description of a user account. Assign this role to assistant administrators responsible for managing user accounts.

Reset Password

Provides all the powers required to reset and modify passwords. Assign this role to assistant administrators responsible for password management.

Reset Password and Unlock Account Using SPA

Provides all the powers required to use Secure Password Administrator to reset passwords and unlock user accounts.

Transform a User

Provides all the powers required to add a user to or remove a user from groups found in a template account, including the ability to modify the user's properties while transforming the user.

User Administration

Provides all the powers required to manage user accounts, associated Microsoft Exchange mailboxes, and group memberships. Assign this role to assistant administrators responsible for managing user accounts.

View All User Properties

Provides all the powers required to view properties for a user account. Assign this role to assistant administrators responsible for auditing user accounts.

WTS Administration

Manage WTS Environment Properties

Provides all the powers required to change the WTS environment properties for a user account. Assign this role to assistant administrators responsible for maintaining the WTS environment or managing user accounts.

Manage WTS Remote Control Properties

Provides all the powers required to change the WTS remote control properties for a user account. Assign this role to assistant administrators responsible for maintaining WTS access or managing user accounts.

Manage WTS Session Properties

Provides all the powers required to change the WTS session properties for a user account. Assign this role to assistant administrators responsible for maintaining WTS sessions or managing user accounts.

Manage WTS Terminal Properties

Provides all the powers required to change the WTS terminal properties for a user account. Assign this role to assistant administrators responsible for maintaining WTS terminal properties or managing user accounts.

WTS Administration

Provides all the powers required to manage Windows Terminal Server (WTS) properties for user accounts in the ActiveView. If you use WTS, assign this role to assistant administrators responsible for maintaining the WTS properties of user accounts.

Accessing Built-in Roles

Access built-in roles to audit the default delegation model or manage your security settings.

To access built-in roles:

- 1 Navigate to **Delegation Management > Manage Roles**.
- 2 Ensure the search field is blank, and click **Find Now** in the **List items that match my criteria** pane.
- 3 Select the appropriate role.

Using Built-in Roles

You cannot delete or modify built-in roles. However, you can incorporate the built-in roles into your existing delegation model or use these roles to design and implement your model.

You can use built-in roles in the following ways:

- ◆ Associate a built-in role with a user account or assistant administrator group. This association provides the user or assistant administrator group members with the appropriate powers for the task.
- ◆ Clone a built-in role and use that clone as the basis for a custom role. You can add other roles or powers to this new role and remove powers originally included in the built-in role.

For more information about designing a dynamic delegation model, see [Understanding the Dynamic Delegation Model](#).

Creating Custom Roles

By creating a role, you can quickly and easily delegate a set of powers that represents an administrative task or workflow. You create and manage roles from the **Delegation Management > Roles** node in the Delegation and Configuration Console. In this node, you can do the following:

- ◆ Create new roles
- ◆ Clone existing roles
- ◆ Modify role properties
- ◆ Delete roles
- ◆ Manage role assignments
 - ◆ Delegate a new assignment
 - ◆ Remove an existing assignment
 - ◆ View properties of an assigned assistant administrator
 - ◆ View properties of an assigned ActiveView
- ◆ Manage the roles and powers in a role (roles can be nested)
- ◆ Generate role change reports

The general workflow to execute any of the actions identified in this section is to select the **Roles** node, and do one of the following:

- ◆ Use the **Tasks** or right-click menu to open the applicable wizard or dialog box to follow through with the necessary action.
- ◆ Find the role object in the **List items that match my criteria** pane, and use the **Tasks** or right-click menu to select and open the applicable wizard or dialog box to follow through with the necessary action.

To execute any of the actions above, you must have the appropriate powers, such as those included in the Manage Security Model role.

9 Powers

Powers are the initial building-blocks for “least privilege” administration. Assigning powers to users helps you implement and maintain your dynamic security model. You perform these procedures in the Delegation and Configuration console.

Built-in Powers

There are over 390 built-in powers for managing objects and performing common administrative tasks that you can work with when defining roles and making delegation assignments. Built-in powers cannot be deleted, but you can clone them to make custom powers. A few examples of built-in powers are included below:

Create Group and Modify All Properties

Provides the power to create groups and specify all properties during group creation.

Delete User Account

If the Recycle Bin is enabled, provides the power to move user accounts to the Recycle Bin. If the Recycle Bin is disabled, provides the power to permanently delete user accounts.

Modify All Computer Properties

Provides the power to modify all properties for computer accounts.

Azure Powers

Use the following powers to delegate the creation and management of Azure users, groups, and contacts.

Azure User Account Powers:

- ◆ Create Azure User and Modify All Properties
- ◆ Delete Azure User Account Permanently
- ◆ Manage Sign-In for Azure Users
- ◆ Manage Sign-In for Azure Users Synced to Azure Tenant
- ◆ Modify All Azure User Properties
- ◆ Reset Azure User Account Password
- ◆ View All Azure User Properties

Azure Group Powers:

- ◆ Add Object to Azure Group
- ◆ Create Azure Group and Modify All Properties
- ◆ Delete Azure Group Account
- ◆ Modify All Azure Group Properties

- ◆ Remove Object from Azure Group
- ◆ View All Azure Group Properties

Azure Contact Powers:

- ◆ Create Azure Contact and Modify All Properties
- ◆ Delete Azure Contact Account
- ◆ Modify All Azure Contact Properties
- ◆ View All Azure Contact Properties

Azure Guest User Account Power:

- ◆ Invite Azure Guest User

The powers that are listed for Azure user accounts also apply to Azure guest user accounts.

To manage granular level properties for Azure objects, you can create custom powers by selecting specified object attributes.

Implementing Custom Powers

To create a custom power, you create a new power or clone an existing power. You can use an existing power as a template for new power delegations. A power defines the properties of an object an assistant administrator can view, modify, or create in your managed domain or subtree. Custom powers can include access to multiple properties, such as the *View All User Properties* power.

NOTE: It is not possible to clone all the built-in powers.

You implement custom powers from the **Delegation Management > Powers** node in the Delegation and Configuration Console. In this node, you can do the following:

- ◆ View all power properties
- ◆ Create new powers
- ◆ Clone existing powers
- ◆ Modify custom powers
- ◆ Generate power change reports

To do these actions, you must have the appropriate powers, such as those included in the Manage Security Model role.

Consider the following process before attempting to create a new power.

1. Review the powers supplied with DRA.
2. Decide whether you need a custom power. If applicable, you can clone an existing custom power.
3. Complete the appropriate wizard-driven procedures. For example, complete the New Power wizard.
4. View your new power.
5. Modify your new power, if necessary.

The general workflow to execute any of the actions identified in this section is to select the **Powers** node, and do one of the following:

- ◆ Use the Tasks or right-click menu to open the applicable wizard or dialog box to follow through with the necessary action.
- ◆ Find the power object in the **List items that match my criteria** pane, and use the **Tasks** or right-click menu to select and open the applicable wizard or dialog box to follow through with the necessary action.

Extending Powers

You can add permissions or functionality to a power by extending that power.

For example, to allow an assistant administrator to create a user account, you can assign either the *Create User and Modify All Properties* power or the *Create User and Modify Limited Properties* power. If you also assign the *Add New User to Group* power, the assistant administrator can add this new user account to a group while using the Create User wizard. In this case, the *Add New User to Group* power provides an additional wizard feature. The *Add New User to Group* power is the **extension power**.

Extension powers cannot add permissions or functionality by themselves. To successfully delegate a task that includes an extension power, you must assign the extension power along with the power you want to extend.

NOTE

- ◆ To successfully create a group and include the new group in an ActiveView, you must have the *Add New Group to ActiveView* power in the specified ActiveView. The specified ActiveView must also include the OU or built-in container that will contain the new group.
 - ◆ To successfully clone a group and include the new group in an ActiveView, you must have the *Add Cloned Group to ActiveView* power in the specified ActiveView. The specified ActiveView must also include the source group as well as the OU or built-in container that will contain the new group.
-

The following table lists some examples of actions that are configurable when creating a new power or modifying the properties of an existing power:

To Delegate This Task	Assign This Power	And This Extension Power
Clone a group and include the new group in a specified ActiveView	Clone Group and Modify All Properties	Add Cloned Group to ActiveView
Create a group and include the new group in a specified ActiveView	Create Group and Modify All Properties	Add New Group to ActiveView
Create a mail enabled contact	Create Contact and Modify All Properties Create Contact and Modify Limited Properties	Enable Email for New Contact

To Delegate This Task	Assign This Power	And This Extension Power
Create a mail enabled group	Create Group and Modify All Properties	Enable Email for New Group
Create a mail enabled user account	Create User and Modify All Properties Create User and Modify Limited Properties	Enable Email for New User
Create a user account and add the new account to specific groups	Create User and Modify All Properties Create User and Modify Limited Properties	Add New User to Group

10 Delegation Assignments

You manage delegation assignments from the **Delegation Management > Assistant Admin** node in the Delegation and Configuration Console. In this node, you can view the powers and roles assigned to assistant administrators and manage the assignments of roles and ActiveViews. You can also do the following with Assistant Admin groups:

- ◆ Add group members
- ◆ Create groups
- ◆ Clone groups
- ◆ Delete groups
- ◆ Modify group properties

To view and manage assignments and update Assistant Admin groups, you must have the appropriate powers, such as those included in the Manage Security Model role.

The general workflow to execute any of the actions identified in this section is to select the **Assistant Admins** node, and do one of the following:

- ◆ Use the **Tasks** or right-click menu to open the applicable wizard or dialog box to follow through with the necessary action.
- ◆ Find the group or assistant administrator in the **List items that match my criteria** pane, and use the **Tasks** or right-click menu to select and open the applicable wizard or dialog box to follow through with the necessary action.

IV Component and Process Configuration

This chapter provides information for configuring DRA for the first time including servers and server customizations, consoles and console customizations, Azure administration, Public Folder administration, and connecting to servers.

- ♦ [Chapter 11, “Initial Configuration,” on page 87](#)
- ♦ [Chapter 12, “Connecting Managed Systems,” on page 121](#)

11 Initial Configuration

This section outlines the required configuration steps if you are installing Directory and Resource Administrator for the first time.

- ♦ “Configuration Checklist” on page 87
- ♦ “Installing or Upgrading Licenses” on page 88
- ♦ “Configure DRA Servers and Features” on page 88
- ♦ “Configuring Change History Reporting” on page 104
- ♦ “Configuring DRA Services for a Group Managed Service Account” on page 111
- ♦ “Configure the Delegation and Configuration Client” on page 112
- ♦ “Configuring the Web Client” on page 112

Configuration Checklist

Use the following checklist to guide you in configuring DRA for first-time use.

Steps	Details
Install a DRA license	Use the Health Check Utility to apply a DRA license. For more information about DRA licenses, see Licensing Requirements .
Configure DRA servers and features	Configure the MMS, clone exceptions, file replication, Event Stamping, caching, AD LDS, dynamic groups, the Recycle Bin, reporting, Unified Change History, and the Workflow Server.
Configure Change History Reporting (optional)	Configure Change History Reporting if you want to integrate with a Change Guardian Server to collect change history data for user events both internal and external to DRA.
Configure DRA Services for a gMSA account (optional)	Configure DRA Services for a group Managed Service Account (gMSA) if you want to manage authentication protocol over multiple servers versus a single server.
Configure the Delegation and Configuration Client	Configure how items are accessed and displayed in the Configuration and Delegation Client.
Configure the Web Client	Configure Auto Logout, certificates, server connections, and authentication components

Installing or Upgrading Licenses

DRA requires a license key file. This file contains your license information and is installed on the Administration server. After you install the Administration server, use the Health Check Utility to install your purchased license. If needed, a trial license key file (`TrialLicense.lic`) is also provided with the installation package that enables you to manage an unlimited number of user accounts and mailboxes for 30 days.

To upgrade an existing or trial license, open the Delegation and Configuration Console, and navigate to **Configuration Management > Update License**. When you upgrade your license, upgrade the license file on each Administration server.

You can view your product license in the Delegation and Configuration Console. To view your product license, navigate to **File menu > DRA Properties > License**.

Configure DRA Servers and Features

Managing least privilege access for Active Directory tasks using DRA has many components and processes that need to be configured. These include general and client component configurations. This section provides information on the general components and processes that need to be configured for DRA.

- ◆ [“Configuring the Multi-Master Set” on page 89](#)
- ◆ [“Managing Clone Exceptions” on page 91](#)
- ◆ [“File Replication” on page 91](#)
- ◆ [“Azure Sync” on page 94](#)
- ◆ [“Enabling Multiple Managers for Groups” on page 94](#)
- ◆ [“Encrypted Communications” on page 95](#)
- ◆ [“Defining Virtual Attributes” on page 95](#)
- ◆ [“Configuring Caching” on page 96](#)
- ◆ [“Enabling Active Directory Printers Collection” on page 99](#)
- ◆ [“AD LDS” on page 99](#)
- ◆ [“Dynamic Group” on page 99](#)
- ◆ [“Configuring the Recycle Bin” on page 99](#)
- ◆ [“Reporting Configuration” on page 100](#)
- ◆ [“Delegating Workflow Automation Server Configuration Powers” on page 102](#)
- ◆ [“Configuring the Workflow Automation Server” on page 103](#)
- ◆ [“Delegating the LDAP Search Powers” on page 103](#)

Configuring the Multi-Master Set

An MMS environment uses multiple Administration servers to manage the same set of domains and member servers. An MMS consists of one primary Administration server and multiple secondary Administration servers.

The default mode for the Administration server is Primary. As you add secondary servers to your MMS environment, keep in mind that a secondary Administration server can belong to only one server set.

To ensure that each server in the set is managing the same data, periodically synchronize the secondary servers with the primary Administration server. To reduce maintenance, use the same service account for all Administration servers in the domain forest.

IMPORTANT

- ◆ While installing the secondary server, select **Secondary Administration Server** in the installer.
 - ◆ The DRA version of the new secondary must be the same as the primary DRA server so that all features that are available in the primary server will be available in the secondary server.
-
- ◆ [“Adding a Secondary Administration Server” on page 89](#)
 - ◆ [“Promoting a Secondary Administration Server” on page 90](#)
 - ◆ [“Demoting a Primary Administration Server” on page 90](#)
 - ◆ [“Scheduling Synchronization” on page 91](#)

Adding a Secondary Administration Server

You can add a secondary Administration server to an existing MMS in the Delegation and Configuration client.

NOTE: To successfully add a new secondary server, you must first install the Directory and Resource Administrator product on the Administration server computer. For more information, see [Install the DRA Administration Server](#).

To add a secondary Administration server:

- 1 Right-click **Administration Servers** in the Configuration Management node and select **Add Secondary Server**.
- 2 In the Add Secondary Server Wizard, click Next.
- 3 In the Secondary server tab, specify the name of the secondary Administration server that you want to add to the MMS.
- 4 In the Access account tab, specify a service account of the secondary Administration server. DRA uses this account only to add the secondary Administration server to the MMS.
- 5 In the Multi-Master access account tab, specify an access account to be used by the primary Administration server for MMS operations. It is recommended not to use the service account of the secondary Administration server as the Multi-Master access account. You can specify any user account from the domain associated with the secondary Administrator server. The Multi-Master access account must be a part of the Local Administrators group on the secondary

server. If the Multi-Master access account does not have sufficient privileges to perform MMS operations, DRA Server automatically delegates the required powers to the Multi-Master access account.

Promoting a Secondary Administration Server

You can promote a secondary Administration server to a primary Administration server. When you promote a secondary Administration server to a primary Administration server, the existing primary Administration server becomes a secondary Administration server in the server set. To promote a secondary Administration server, you must have the appropriate powers, such as those included in the built-in Configure Servers and Domains role. Before promoting a secondary Administration server, synchronize the MMS so that it has the latest configuration.

For information about synchronizing the MMS, see [Scheduling Synchronization](#).

NOTE: A newly promoted primary server can only connect to secondary servers that were available during the promotion process. If a secondary server became unavailable during the promotion process, contact Technical Support.

To promote a secondary Administration server:

- 1 Navigate to **Configuration Management > Administration Servers** node.
- 2 In the right pane, select the secondary Administration server you want to promote.
- 3 On the Tasks menu, click **Advanced > Promote Server**.

IMPORTANT: When the Service account of the Secondary Server is different from the Primary Server or the Secondary Server is installed in a different domain than the Primary Server (Trusted domains/untrusted domains), and you promote the Secondary Server, ensure you delegate the following roles before promoting the Secondary Server: **Audit All Objects**, **Configure Servers and Domains**, and **Generate UI Reports**. Then verify that the MMS synchronizations succeeded.

Demoting a Primary Administration Server

You can demote a primary Administration server to a secondary Administration server. To demote a primary Administration server, you must have the appropriate powers, such as those included in the built-in Configure Servers and Domains role.

To demote a primary Administration server:

- 1 Navigate to **Configuration Management > Administration Servers** node.
- 2 In the right pane, select the primary Administration server you want to demote.
- 3 On the Tasks menu, click **Advanced > Demote Server**.
- 4 Specify the computer you want to designate as the new primary Administration server, and click **OK**.

Scheduling Synchronization

Synchronization ensures that all Administration servers in the MMS use the same configuration data. Although you can manually synchronize servers at any time, the default schedule is set to synchronize the MMS every 4 hours. You modify this schedule to tailor it to your enterprise needs.

To modify the synchronization schedule or to manually synchronize MMS servers, you must have the appropriate powers, such as those included in the built-in Configure Servers and Domains role.

To access the synchronization schedule or for manual syncs, navigate to **Configuration Management > Administration Servers** and use the **Tasks** menu or right-click options on a selected server. The synchronization schedule is in a selected server's Properties.

Understanding synchronization options

There are four different options for synchronizing MMS servers:

- ◆ Select the primary server and synchronize all secondary servers "Synchronize All Servers"
- ◆ Select a secondary server and synchronize just that server
- ◆ Configure the synchronization schedule for primary and secondary servers independently
- ◆ Configure the synchronization schedule for all servers. This option is enabled when you have the following setting selected in the primary server synchronization schedule:

Configure secondary Administration servers when refreshing the primary Administration server

NOTE: If you uncheck this option, the configuration files are copied to the secondary servers on the primary schedule but they will not be loaded by the secondary at that time; they will be loaded based on the schedule configured on the secondary server. This is useful if the servers are in different time zones. For example, you could configure all servers to refresh their configuration in the middle of the night, even though that may be a different time because of time zones.

Managing Clone Exceptions

Clone exceptions enable you to define properties for users, groups, contacts, and computers that will not be copied when one of these objects is cloned.

With the appropriate powers, you can manage clone exceptions. The Manage Clone Exceptions role grants powers to view, create, and delete clone exceptions.

To view or delete an existing clone exception, or to create a new clone exception, navigate to **Configuration Management > Clone Exceptions > Tasks** or right-click menu.

File Replication

When you create custom tools, you may need to install supporting files used by the custom tool on the DRA Delegation and Configuration Console computer before the custom tool can run. You can use DRA file replication capabilities to replicate custom tool support files quickly and easily from the

primary Administration server to secondary Administration servers in the MMS, as well as to DRA client computers. File replication can also be used to replicate trigger scripts from primary to secondary servers.

Custom Tools and File Replication features are only available in the Delegation and Configuration Console.

You can use custom tools and file replication together to ensure DRA client computers can access custom tool files. DRA replicates custom tool files to secondary Administration servers to ensure DRA client computers connecting to secondary Administration servers can access custom tools.

DRA replicates the custom tool files on the primary Administration server to secondary Administration servers during the MMS synchronization process. DRA downloads the custom tool files to DRA client computers when the DRA client computers connect to the Administration servers.

NOTE: DRA downloads the custom tool files to the following location on the DRA client computers:

`{DRAInstallDir}\{MMS ID}\Download`

MMSID is the identification of the Multi-Master Set from which DRA downloads the custom tool files.

- ♦ [“Uploading Custom Tool Files for Replication” on page 92](#)
- ♦ [“Replicating Multiple Files Between Administration Servers” on page 93](#)
- ♦ [“Replicating Multiple Files to DRA Client Computers” on page 93](#)

Uploading Custom Tool Files for Replication

When you upload files to the primary Administration server, you specify the files you want to upload and replicate between the primary Administration server and all secondary Administration servers in the MMS set. DRA allows you to upload library files, script files and executable files.

The Replicate Files role allows you to replicate files from the primary Administration server to the secondary Administration servers in the MMS as well as DRA client computers. The Replicate File role contains the following powers:

- ♦ **Delete Files from Server:** This power enables DRA to delete files that no longer exist on the primary Administration server, on secondary Administration servers, and on DRA client computers.
- ♦ **Set File Information:** This power enables DRA to update file information for files on secondary Administration servers.
- ♦ **Upload Files to Server:** This power enables DRA to upload files from the DRA client computer to the primary Administration server.

NOTE: You can upload only one file for replication at a time using the File Replication user interface in the Delegation and Configuration Console.

To upload a custom tool file to the primary Administration server:

- 1 Navigate to **Configuration Management > File Replication**.
- 2 On the Tasks menu, click **Upload File**.

- 3 To search for and select the file you want to upload, click **Browse**.
- 4 If you want to download the selected file to all DRA client computers, select the **Download to all client computers** check box.
- 5 If you want to register a COM library, select the **Register COM library** check box.
- 6 Click **OK**.

NOTE

- ◆ DRA uploads the script file or supporting files that need to be replicated to other secondary Administration servers to `{DRAInstallDir}\FileTransfer\Replicate` folder in the primary Administration server. The `{DRAInstallDir}\FileTransfer\Replicate` folder is also referred as `{DRA_Replicated_Files_Path}`.
 - ◆ DRA uploads the script file or supporting files that need to be replicated to DRA client computers to `{DRAInstallDir}\FileTransfer\Download` folder in the primary Administration server.
 - ◆ The custom tool file uploaded to the primary Administration server is distributed to secondary Administration servers during the next scheduled synchronization or by manual synchronization.
-

Replicating Multiple Files Between Administration Servers

If you have multiple files you want to upload and replicate between the primary Administration server and secondary Administration servers in your MMS, you can manually upload these files for replication by copying the files to the primary Administration server replication directory, which is in the following location:

```
{DRAInstallDir}\FileTransfer\Replicate
```

The replication directory is created when DRA is installed.

The Administration server automatically identifies the files in the replication directory and replicates the files between Administration servers during the next scheduled synchronization. After synchronization, DRA displays the uploaded files in the File Replication window in the Delegation and Configuration console.

NOTE: If you want to replicate files that contain COM libraries that must be registered, you cannot manually copy the files to the Administration server replication directory. You must use the Delegation and Configuration console to upload each file and register the COM library.

Replicating Multiple Files to DRA Client Computers

If you have multiple files you want to replicate between the primary Administration server and DRA client computers, you can copy the files to the client replication directory on the primary Administration server, which is in the following location:

```
{DRAInstallDir}\FileTransfer\Download
```

The client replication directory is created when DRA is installed.

The Administration server automatically identifies the files in the `Download` folder and replicates the files to the secondary Administration servers during the next scheduled synchronization. After synchronization, DRA displays the uploaded files in the File Replication window in the Delegation and Configuration console. DRA downloads the replicated files to the DRA client computers the first time the DRA client computers connect to the Administration servers after replication.

NOTE: If you want to replicate files that contain COM libraries that must be registered, you cannot copy the files into the Administration server download directory. You must use the Delegation and Configuration console to upload each file and register the COM library.

Azure Sync

Azure Sync enables you to enforce invalid characters and character length policies to prevent directory synchronization failures. Selecting this option will ensure that any properties that are synchronized with Azure Active Directory will restrict invalid characters and enforce character length limits.

To enable Azure Sync:

- 1 In the left pane, click **Configuration Management**.
- 2 Under Common Tasks in the right pane, click **Update Administration Server Options**.
- 3 On the Azure Sync tab, select **Enforce online mailbox policies for invalid characters and character length**.

Enabling Multiple Managers for Groups

When you enable support for multiple managers to manage a group, one of two default attributes is used to store the group's managers. The attribute when running Microsoft Exchange is the `msExchCoManagedByLink` attribute. The default attribute when not running Microsoft Exchange is the `nonSecurityMember` attribute. The latter option can be modified. However, we recommend that you contact Technical Support to determine an appropriate attribute if you need to change this setting.

To enable multiple manager support for groups:

- 1 In the left pane, click **Configuration Management**.
- 2 Under Common Tasks in the right pane, click **Update Administration Server Options**.
- 3 On the Enable Support for Group Multiple Managers tab, select the **Enable support for group's multiple managers** check box.

Encrypted Communications

This function allows you to enable or disable the use of encrypted communication between the Delegation and Configuration client and the Administration server. By default, DRA encrypts account passwords. This feature does not encrypt Web Client or PowerShell communications, which is handled separately by server certificates.

Using encrypted communications can impact performance. Encrypted communication is disabled by default. If you enable this option, data is encrypted during communication between the user interfaces and the Administration server. DRA uses the Microsoft standard encryption for Remote Procedure Call (RPC).

To enable encrypted communications, navigate to **Configuration Management > Update Administration Server Options > General** tab and select the **Encrypted Communications** check box.

NOTE: To encrypt all communications between the Administration server and user interfaces, you must have the appropriate powers, such as those in the built-in Configure Servers and Domains role.

Defining Virtual Attributes

Using virtual attributes, you can create new properties and associate these properties with users, groups, Dynamic Distribution groups, contacts, computers, and OUs. Virtual attributes allow you to create new properties without requiring you to extend the Active Directory schema.

Using virtual attributes, you can add new properties to objects in Active Directory. You can only create, enable, disable, associate, and disassociate virtual attributes on the primary Administration server. DRA stores the virtual attributes you create in AD LDS. DRA replicates virtual attributes on the primary Administration server to secondary Administration servers during the MMS synchronization process.

With the appropriate powers, you can manage virtual attributes. The Manage Virtual Attributes role grants powers to create, enable, associate, disassociate, disable, and view virtual attributes.

- ◆ [“Creating Virtual Attributes” on page 95](#)
- ◆ [“Associating Virtual Attributes with Objects” on page 96](#)
- ◆ [“Disassociating Virtual Attributes” on page 96](#)
- ◆ [“Disabling Virtual Attributes” on page 96](#)

Creating Virtual Attributes

You need the *Create Virtual Attributes* power to create virtual attributes and the *View Virtual Attributes* power to view virtual attributes.

To create a virtual attribute, navigate to **Configuration Management > Virtual Attributes > Managed Attributes** node, and click **New Virtual Attribute** in the Tasks menu.

Associating Virtual Attributes with Objects

You can associate only enabled virtual attributes with Active Directory objects. Once you associate a virtual attribute with an object, the virtual attribute is available as part of the object properties.

To expose virtual attributes through the DRA user interfaces, you need to create a custom property page.

To associate a virtual attribute with an object, navigate to **Configuration Management > Virtual Attributes > Managed Attributes** node, right-click the virtual attribute you want to use, and select **Associate > (object type)**.

NOTE

- ◆ You can only associate virtual attributes with users, groups, dynamic distribution groups, computers, contacts, and OUs.
 - ◆ When you associate a virtual attribute with an object, DRA automatically creates two default custom powers. Assistant administrators require these custom powers to manage the virtual attribute.
-

Disassociating Virtual Attributes

You can disassociate virtual attributes from Active Directory objects. Any new object that you create does not display the disassociated virtual attribute as part of the object properties.

To disassociate a virtual attribute from an Active Directory object, navigate to **Configuration Management > Virtual Attributes > Managed Classes > (object type)** node. Right-click the virtual attribute, and select **Disassociate**.

Disabling Virtual Attributes

You can disable virtual attributes if they are not associated with an Active Directory object. When you disable a virtual attribute, administrators cannot view or associate the virtual attribute with an object.

To disable a virtual attribute, navigate to **Configuration Management > Managed Attributes**. Right-click the desired attribute in the list pane, and select **Disable**.

Configuring Caching

The Administration server builds and maintains an **accounts cache** that contains portions of the Active Directory for the managed domains. DRA uses the accounts cache to improve performance when managing user accounts, groups, contacts, and computer accounts.

To schedule a cache refresh time or view the cache status, you must have the appropriate powers, such as those included in the built-in Configure Servers and Domains role.

NOTE: To perform incremental accounts cache refreshes in domains that contain managed subtrees, ensure the service account has read access to the Deleted Objects container as well as all objects in the domain of the subtree. You can use the Deleted Objects Utility to verify and delegate the appropriate permissions.

- ♦ [“Full and Incremental Refreshes” on page 97](#)
- ♦ [“Default Scheduled Times” on page 98](#)

Full and Incremental Refreshes

An incremental accounts cache refresh updates only the data that changed since the last refresh. The incremental refresh provides a streamlined way to keep up with your changing Active Directory. Use the incremental refresh to quickly update the accounts cache while incurring the least impact on your enterprise.

IMPORTANT: Microsoft Server limits the number of concurrent users connected to the WinRM/WinRS session to five and the number of shells per user to five, so ensure that the same user account is limited to five shells for DRA secondary servers.

An incremental refresh updates the following data:

- ♦ New and cloned objects
- ♦ Deleted and moved objects
- ♦ Group memberships
- ♦ All cached object properties for modified objects

A full accounts cache refresh rebuilds DRA’s accounts cache for the specified domain.

NOTE: While a Full Accounts Cache Refresh is running, the domain will be unavailable to DRA users.

Performing a Full Accounts Cache Refresh

To refresh the accounts cache, you must have the appropriate powers, such as those included in the built-in “Configure Servers and Domains” role.

To perform an immediate full accounts cache refresh:

- 1 Navigate to **Configuration Management > Managed Domains**.
- 2 Right-click the desired domain, and select **Properties**.
- 3 Click **Refresh Now** in the **Full refresh** tab.

Default Scheduled Times

How often you should refresh the accounts cache depends on how often your enterprise changes. Use the incremental refresh to update the accounts cache often, ensuring that DRA has the most up to date information about the Active Directory.

By default, the Administration server performs an incremental accounts cache refresh at the following times:

Domain Type	Default Scheduled Refresh Time
Managed Domains	Every 5 minutes
Trusted Domains	Every hour
Azure Tenant	Every 15 minutes

You cannot schedule a FACR; however, DRA runs an automatic FACR under the following circumstances:

- ◆ After you configure a managed domain for the first time.
- ◆ After you upgrade DRA to a new full version from a previous version.
- ◆ After you install a DRA service pack.

Performing a full accounts cache refresh can require several minutes.

Considerations

You must periodically refresh the accounts cache to ensure DRA has the latest information. Before performing or scheduling an accounts cache refresh, review the following considerations:

- ◆ To perform an incremental accounts cache refresh, the Administration server service account or access account must have permission to access deleted objects in the Active Directory of the managed or trusted domain.
- ◆ When DRA performs an accounts cache refresh, the Administration server does not include domain local security groups from trusted domains. Because the cache does not contain these groups, DRA does not allow you to add a domain local security group from the trusted domain to a local group on the managed member server.
- ◆ If you omit a trusted domain from an accounts cache refresh, the Administration server also omits that domain from the domain configuration refresh.
- ◆ If you include a previously omitted trusted domain in the accounts cache refresh, perform a full accounts cache refresh for the managed domain. This ensures that the accounts cache on the Administration server for the managed domain correctly reflects group membership data in your managed and trusted domains.
- ◆ If you set the incremental accounts cache refresh interval to **Never**, the Administration server performs full accounts cache refreshes only. A full account cache refresh may take some time, during which you cannot manage objects in this domain.

- ♦ DRA cannot automatically determine when changes are made through other tools, such as Microsoft Directory Services. Operations performed outside DRA can affect the accuracy of the cached information. For example, if you use another tool to add a mailbox to a user account, you cannot use Exchange to manage this mailbox until you update the accounts cache.
- ♦ Performing a full accounts cache refresh deletes the last logon statistics maintained in the cache. The Administration server then collects the latest logon information from all the domain controllers.

Enabling Active Directory Printers Collection

The AD Printers collection is disabled by default. To enable it, navigate to **Configuration Management > Update Administration Server Options > General** tab, and select the Collect Printers check box.

AD LDS

You can configure the AD LDS cleanup refresh to run on a schedule for specific domains. The default setting is “Never” refresh. You can also view the cleanup status and view specific information related to the AD LDS (ADAM) configuration.

To configure the schedule or view the status for AD LDS Cleanup, right-click the desired domain in the **Account and Resource Management > All My Managed Objects** node, and select **Properties > Adlds Cleanup Refresh Schedule** or **Adlds Cleanup status**, respectively.

To view the AD LDS (ADAM) configuration information, navigate to **Configuration Management > Update Server Options > ADAM Configuration**.

Dynamic Group

A dynamic group is one whose membership changes based on a defined set of criteria that you configure in the group’s properties. In Domain Properties, you can configure the Dynamic Group refresh to run on a schedule for specific domains. The default setting is “Never” refresh. You can also view the refresh status.

To configure the schedule or view the status for Dynamic Group refresh, right-click the desired domain in the **Account and Resource Management > All My Managed Objects** node, and select **Properties > Dynamic group refresh** or **Dynamic group status**, respectively.

For more information about dynamic groups, see [DRA Dynamic Groups](#).

Configuring the Recycle Bin

You can enable or disable the Recycle Bin for each Microsoft Windows domain or objects within each domain and configure when and how you want Recycle Bin cleanup to occur.

For detailed information about using the Recycle Bin, see [Recycle Bin](#).

Enabling the Recycle Bin

You can enable the Recycle Bin for specific Microsoft Windows domains and objects within those domains. By default, DRA enables the Recycle Bin for each domain it manages and all the domain's objects. You must be a member of the DRA Admins or DRA Configuration Admins group to enable the Recycle Bin.

If your environment includes the following configuration, use the Recycle Bin Utility to enable this feature:

- ♦ DRA is managing a subtree of this domain.
- ♦ The Administration server service or access account does not have permission to create the Recycle Bin container, move accounts to this container, and modify accounts in this container.

You can also use the Recycle Bin Utility to verify the Administration server service or access account permissions on the Recycle Bin container.

To enable the Recycle Bin, right-click the desired domain in the **Recycle Bin** node, and select **Enable Recycle Bin**.

Disabling the Recycle Bin

You can disable the Recycle Bin for specific Microsoft Windows domains and objects within those domains. If a disabled Recycle Bin contains accounts, you cannot view, permanently delete, or restore these accounts.

You must be a member of the DRA Admins or DRA Configuration Admins assistant administrator group to disable the Recycle Bin.

To disable the Recycle Bin, right-click the desired domain in the **Recycle Bin** node, and select **Disable Recycle Bin**.

Configuring Recycle Bin Objects and Cleanup

The default setting for Recycle Bin cleanup is daily. You can change this configuration to clean up the domain Recycle Bin every x days. During the scheduled cleanup, the Recycle Bin deletes objects that are older than the number of days you have configured for each object type. The default setting for each type is to delete objects older than 1 day. You can customize the behavior of Recycle Bin cleanup by disabling, re-enabling, and setting the age of objects for deletion for each object type.

To configure Recycle Bin cleanup, select the desired domain in the Delegation and Configuration console and go to **Tasks > Properties > Recycle Bin** tab.

Reporting Configuration

The following sections provide conceptual information about DRA Management reports and the report collectors that you can enable. To access the wizard where you can configure the collectors, navigate to **Configuration Management > Update Reporting Service Configuration**.

Configuring the Active Directory Collector

The Active Directory Collector collects a specified set of attributes from Active Directory for each managed user, group, contact, computer, OU, and Dynamic Distribution group in DRA. These attributes are stored in the reporting database and are used to generate reports in the Reporting Console.

You can configure the Active Directory Collector to specify which attributes are collected and stored in the reporting database. You can also configure which DRA Administration server the collector will run on.

Configuring the DRA Collector

The DRA Collector collects information about your DRA configuration and stores that information in the reporting database, which is used to generate reports in the Reporting Console.

To enable the DRA Collector, you must specify which DRA Administration server the collector will run on. As a best practice, you should schedule the DRA Collector to run after the Active Directory Collector successfully runs and during times when the server is least loaded or outside of normal working hours.

Configuring the Azure Tenant Collector

The Azure Tenant Collector collects tenant information, Office 365 mailbox details, and mailbox permissions for synced users and stores this information in the reporting database, which is used to generate reports in the Reporting Console.

To enable the Azure Tenant Collector, you must specify which DRA Administration server the collector will run on.

NOTE

- ◆ From 10.2.2, tenant collector can be configured and data can be collected only if the tenant is managed with certificate-based authentication type as basic authentication is no longer supported.
 - ◆ The Azure tenant can only run a successful collection after its corresponding domain's Active Directory Collector runs a successful collection.
-

Configuring the Management Reports Collector

The Management Reports Collector collects DRA audit information and stores that information in the reporting database, which is used to generate reports in the Reporting Console. When you enable the collector, you can configure how often the data is updated in the database for queries run in the DRA Reporting tool.

This configuration requires that the DRA Service account has the **sysadmin** permission in SQL Server on the Reporting server. The configurable options are defined below:

- ♦ **Audit Export Data Interval:** This is the time interval when Audit data from the DRA trace log (LAS) is exported to the "SMCubeDepot" database in SQL Server.
- ♦ **Management Report Summarization Interval:** This is the time interval when Audit data from the SMCubeDepot database is pumped into the DRA Reporting database where it can be queried by the DRA Reporting tool.

Gathering Last Logon Statistics

You can configure DRA to collect last logon statistics from all domain controllers in the managed domain. To enable and schedule the last logon statistics gathering, you must have the appropriate powers, such as those included in the built-in Configure Servers and Domains role.

By default, the last logon statistics gathering feature is disabled. If you want to gather last logon statistic data, you must enable this feature. Once you enable last logon statistics gathering, you can view last logon statistics for a particular user or display the status of the last logon statistics gathering.

To gather last logon statistics:

- 1 Navigate to **Configuration Management > Managed Domains**.
- 2 Right-click the desired domain, and select **Properties**.
- 3 Click the **Last logon schedule** tab to configure last logon statistics collection.

Delegating Workflow Automation Server Configuration Powers

To manage Workflow, assign the Workflow Automation Server Administration role or the applicable powers below to assistant administrators:

- ♦ Create Workflow Event and Modify All Properties
- ♦ Delete Workflow Automation Server Configuration
- ♦ Set Workflow Automation Server Configuration Information
- ♦ Start Workflow
- ♦ View All Workflow Event Properties
- ♦ View All Workflow Properties
- ♦ View Workflow Automation Server Configuration Information

To delegate Workflow Automation server configuration powers:

- 1 Click **Powers** in the Delegation Management node, and use the search objects feature to find and select the Workflow powers that you want.
- 2 Right-click one of the selected Workflow powers and select **Delegate Roles and Powers**.
- 3 Search for the specific user, group, or assistant administrator group that you want to delegate powers to.
- 4 Use the **Object Selector** to find and add the objects that you want, and then click **Roles and Powers** in the **Wizard**.
- 5 Click **ActiveViews**, and use the **Object Selector** to find and add the ActiveViews that you want.
- 6 Click **Next** and then **Finish** to complete the delegation process.

Configuring the Workflow Automation Server

To use Workflow Automation in DRA, you must install the Workflow Automation Engine on a Windows Server and then configure the Workflow Automation server through the Delegation and Configuration console.

To configure the Workflow Automation server:

- 1 Log in to the Delegation and Configuration Console.
For Workflow Automation powers, see [Delegating Workflow Automation Server Configuration Powers](#).
- 2 Expand **Configuration Management > Integration Servers**.
- 3 Right-click **Workflow Automation**, and select **New Workflow Automation Server**.
- 4 In the **Add Workflow Automation Server** wizard, specify the details such as server name, port, protocol, and access account.
- 5 Test the server connection, and click **Finish** to save the configuration.

For information on installing the Workflow Automation Engine, see the *Workflow Automation Administrator Guide* on the [DRA Documentation site](#).

Delegating the LDAP Search Powers

DRA enables you to search for LDAP objects in on-premises Active Directory domains such as users, contacts, computers, groups, and OUs from the LDAP server. The DRA server still handles the operation and it is the domain controller where the search is executed. Use the search filters for more efficient and effective searches. Also, you can save the search query for future use and it can be shared as a public query or you can use it for your own by marking it as private. You can edit the saved queries.

The LDAP Advanced Queries role grants assistant administrators the powers to create and manage LDAP Search queries.

Use the following powers to delegate the creation and management of LDAP Search queries:

- ♦ Create Private Advanced Query
- ♦ Create Public Advanced Query

- ◆ Delete Public Advanced Query
- ◆ Execute Advanced Query
- ◆ Execute Save Advanced Query
- ◆ Modify Public Query
- ◆ View Advanced Query

To delegate LDAP Query powers:

- 1 Click **Powers** in the Delegation Management node, and use the search objects feature to find and select the Advanced LDAP Queries powers that you want.
- 2 Right-click one of the selected LDAP powers and select **Delegate Roles and Powers**.
- 3 Search for the specific user, group, or assistant administrator group that you want to delegate powers to.
- 4 Use the **Object Selector** to find and add the objects that you want, and then click **Roles and Powers** in the **Wizard**.
- 5 Click **ActiveViews**, and use the **Object Selector** to find and add the ActiveViews that you want.
- 6 Click **Next** and then **Finish** to complete the delegation process.

To access the search feature in the Web Console, navigate to **Management > LDAP Search**.

Configuring Change History Reporting

DRA enables delegation of managed changes in an enterprise organization and Change Guardian (CG) enables monitoring for managed and unmanaged changes occurring in Active Directory. Integrating DRA and CG provides:

- ◆ Ability to see DRA delegated Assistant Administrator that made a change to Active Directory in CG events for changes made through DRA.
- ◆ Ability to see recent change history for an object in DRA of both changes made through DRA and changes captured by CG that originated outside of DRA.
- ◆ Changes made through DRA are designated as “Managed” changes in CG.

To configure DRA change history reporting, follow these steps:

1. [Install the Change Guardian Windows Agent.](#)
2. [Add an Active Directory license key.](#)
3. [Configure Active Directory.](#)
4. [Create and assign an Active Directory policy.](#)
5. [Manage Active Directory domains.](#)
6. [Enable Event Stamping.](#)
7. [Configure Unified Change History.](#)

Once you have completed the steps above for installing Change Guardian and configuring DRA and CG integration, users can generate and view UCH reports in the Web Console.

For more information, see “[Generating Change History Reports](#)” in the *Directory and Resource Administrator User Guide*.

Install the Change Guardian Windows Agent

Before you begin DRA and CG integration, install the Change Guardian Windows Agent. For more information, see the [Change Guardian Installation and Administration Guide](#).

Add an Active Directory License key

You must add licenses for both the Change Guardian server and applications or modules you plan to monitor. For more information, see the [Change Guardian Installation and Administration Guide](#).

Configure Active Directory

To configure Active Directory for Change History, reference the following sections:

Configuring the Security Event Log

Configure the security event log to ensure that Active Directory events remain in the event log until Change Guardian processes them.

To configure the security event log:

- 1 Log in as an administrator to a computer in the domain that you want to configure.
- 2 To open Group Policy Management Console, enter the following at the command prompt:
`gpmmc . msc`
- 3 Open **Forest > Domains > domainName > Domain Controllers**.
- 4 Right-click **Default Domain Controllers Policy**, and then click **Edit**.

NOTE: Changing the default domain controllers policy is important because a GPO linked to the domain controller (DC) organizational unit (OU) with a higher link order can override this configuration when you restart the computer or run `gpUpdate` again. If your corporate standards do not allow you to modify the default domain controllers policy, create a GPO for your Change Guardian settings, add these settings to the GPO, and set it to have the highest link order in the Domain Controllers OU.

- 5 Expand **Computer Configuration > Policies > Windows Settings > Security Settings**.
- 6 Select **Event Log** and set:
 - ♦ **Maximum security log size** to 10240 KB (10 MB) or more
 - ♦ **Retention method for security log** to **Overwrite events as needed**
- 7 To update policy settings, run the `gpUpdate` command at the command prompt.

To verify the configuration is successful:

- 1 Open a command prompt as an administrator to the computer.
- 2 Start Event Viewer: `eventvwr`
- 3 Under Windows logs, right-click **Security**, and select **Properties**.
- 4 Ensure that the settings show maximum log size of 10240 KB (10 MB) or more and that "Overwrite events as needed" is selected.

Configuring AD Auditing

Configure AD auditing to enable logging of AD events in the security event log.

Configure Default Domain Controllers Policy GPO with Audit Directory service access to monitor both success and failure events.

To configure AD auditing:

- 1 Log in as an administrator to a computer in the domain that you want to configure.
- 2 To open Group Policy Management Console, run `gpmc.msc` at the command prompt.
- 3 Expand **Forest > Domains > *domainName* > Domain Controllers**.
- 4 Right-click **Default Domain Controllers Policy**, and click **Edit**.

NOTE: Changing the default domain controllers policy is important because a GPO linked to the domain controller (DC) organizational unit (OU) with a higher link order can override this configuration when you restart the computer or run `gpupdate` again. If your corporate standards do not allow you to modify the default domain controllers policy, create a GPO for your Change Guardian settings, add these settings to the GPO, and set it to have the highest link order in the Domain Controllers OU.

- 5 Expand **Computer Configuration > Policies > Windows Settings > Security Settings > Advanced Audit Policy Configuration > Audit Policies**.
 - 5a To configure AD and Group Policy, under **Account Management**, and **Policy Change**, select the following for each subcategory: **Configure the following audit events, Success, and Failure**.
 - 5b To configure only AD, under **DS Access**, select the following for each subcategory: **Configure the following audit events, Success, and Failure**.
- 6 Expand **Computer Configuration > Policies > Windows Settings > Security Settings > Local Policies > Audit Policy**.
 - 6a For each of the following policies, select **Define these policy settings, Success, and Failure** in the **Security Policy Setting** tab:
 - ♦ **Audit account management**
 - ♦ **Audit directory service access**
 - ♦ **Audit policy change**
 - 7 To update policy settings, run the `gpupdate` command at the command prompt.

For more information, see [Monitoring Active Directory for Signs of Compromise](#) in the Microsoft Documentation site

Configuring User and Group Auditing

Configure user and group auditing to audit the following activities:

- ♦ Logon and logoff activities of local users and Active Directory users
- ♦ Local user settings
- ♦ Local group settings

To configure user and group auditing:

- 1 Log in as an administrator to a computer in the domain that you want to configure.
- 2 Open Microsoft Management Console, select **File > Add/Remove Snap-in**.
- 3 Select **Group Policy Management Editor** and click **Add**.
- 4 In the Select Group Policy Object window, click **Browse**.
- 5 Select **Domain Controllers.FQDN**, where *FQDN* is the Fully Qualified Domain Name for the domain controller computer.
- 6 Select **Default Domain Controllers Policy**.
- 7 In the Microsoft Management Console, expand **Default Domain Controllers Policy FQDN > Computer Configuration > Policies > Windows Settings Security Settings > Local Policies > Audit Policy**.
- 8 Under **Audit Account Logon Events** and **Audit Logon Events**, select **Define these policy settings, Success, and Failure**.
- 9 In the Microsoft Management Console, expand **Default Domain Controllers Policy FQDN > Computer Configuration > Policies > Windows Settings > Security Settings > Advanced Audit Policy Configuration > Audit Policies > Logon/Logoff**.
- 10 Under **Audit Logon**, select **Audit Logon, Success, and Failure**.
- 11 Under **Audit Logoff**, select **Audit Logoff, Success, and Failure**.
- 12 To update policy settings, run the `gpupdate /force` command at the command prompt.

Configuring Security Access Control Lists

To monitor all changes of current and future objects inside Active Directory, configure the domain node.

To configure SACLs:

- 1 Log in as an administrator to a computer in the domain that you want to configure.
- 2 To open ADSI Edit configuration tool, run `adsiedit.msc` at the command prompt.
- 3 Right-click **ADSI Edit**, and select **Connect to**.
- 4 In the Connection Settings window, specify the following:
 - ◆ **Name** as `Default naming context`.
 - ◆ **Path** to the domain to configure.
 - ◆ If you are performing this step for the first time, select **Default naming context**.
 - ◆ If you are performing for the second time, select **Schema**.
 - ◆ If you are performing for the third time, select **Configuration**.

NOTE: You must perform [Step 4](#) through [Step 11](#) three times, to configure connection points for **Default naming context**, **Schema**, and **Configuration**.

- 5 In **Connection Point**, set **Select a well known Naming Context** to **Default naming context**.
- 6 In the ADSI Edit window, expand **Default naming context**.
- 7 Right-click the node under the connection point (begins with `DC=` or `CN=`), and click **Properties**.

- 8 On the **Security** tab, click **Advanced > Auditing > Add**.
- 9 In **Applies to** or **Apply onto**, select **This object and all descendant objects**.
- 10 Configure auditing to monitor every user:
 - 10a Click **Select a principal**, and type **everyone** in **Enter the object name to select**.
 - 10b Specify the following options:
 - ◆ **Type as All**
 - ◆ **Select Permissions as:**
 - ◆ **Write All Properties**
 - ◆ **Delete**
 - ◆ **Modify Permissions**
 - ◆ **Modify Owner**
 - ◆ **Create All Child Objects**
The other nodes related to child objects are selected automatically
 - ◆ **Delete All Child Objects**
The other nodes related to child objects are selected automatically
- 11 Deselect the option **Apply these auditing entries to objects and/or containers within this container only**.
- 12 Repeat [Step 4](#) through [Step 11](#) two more times.

Create and Assign an Active Directory Policy

You can create a fresh policy without preconfigured settings.

To create a policy:

- 1 In Policy Editor, select one of the applications, such as Active Directory.
- 2 Expand the list of policies and select the policy type you want to create. For example, select **Active Directory Policies > AD Object**.
- 3 On the Configuration Policy screen, make the appropriate changes.
- 4 (Conditional) If you want to enable the policy immediately, select **Enable this policy revision now**.

To assign:

- 1 Click **CONFIGURATION > Policies > Assign Policies**.
- 2 (Conditional) To assign to an agent group, click **Agent Groups** and **Default Group** or **Custom Group**, and click on the group name.
- 3 (Conditional) To assign to an agent, click **AGENTS** and select the agent name.
- 4 Click on the icon under **ASSIGN UNASSIGN**.
- 5 Select the policies from either **POLICY SETS**, **POLICIES**, or both, and click **APPLY**.

NOTE: You cannot assign policies using agent groups for the following asset types: Azure AD, AWS for IAM, Dell EMC, Microsoft Exchange, Microsoft Office 365

Manage Active Directory Domains

To configure a domain in DRA as a Managed domain, see [Managing Active Directory Domains](#).

Enable Event Stamping in DRA

When AD Domain Services auditing is enabled, DRA events are logged as having been generated by either the DRA Service account or the Domain Access account if one is configured. Event Stamping takes this feature one step further by generating an additional AD DS event that identifies the assistant administrator who performed the operation.

For these events to be generated you must configure AD DS auditing and enable Event Stamping on the DRA Administration Server. When Event Stamping is enabled, you will be able to view the changes that assistant administrators make in Change Guardian Event reports.

- ◆ To configure AD DS auditing, see the Microsoft documentation on [AD DS Auditing Step-by-Step Guide](#).
- ◆ To configure Change Guardian integration, see [Configuring Unified Change History Servers](#).
- ◆ To enable Event Stamping, open the Delegation and Configuration console as DRA Administrator, and do the following:
 1. Navigate to **Configuration Management > Update Administration Server Options > Event Stamping**.
 2. Select an object type, and click **Update**.
 3. Select an attribute to use for Event Stamping for that object type.

DRA currently supports Event Stamping for users, groups, contacts, computers, and organizational units.

DRA also requires that the attributes exist in the AD schema for each of your managed domains. You should be aware of this if you add managed domains after configuring Event Stamping. If you were to add a managed domain that does not contain a selected attribute, operations from that domain would not be audited with the Event Stamping data.

DRA will be modifying these attributes so you should select attributes that are not used by DRA or any other application in your environment.

For more information about Event Stamping, see [How Event Stamping Works](#).

Configure Unified Change History

The Unified Change History (UCH) Server feature enables you to generate reports for changes made outside of DRA.

Delegating the Unified Change History Server Configuration Powers

To manage Unified Change History Server, assign the Unified Change History Server Administration role or the applicable powers below to assistant administrators:

- ◆ Delete Unified Change History Server Configuration

- ◆ Set Unified Change History Configuration Information
- ◆ View Unified Change History Configuration Information

To delegate Unified Change History Server powers:

- 1 Click **Powers** in the Delegation Management node, and use the search objects feature to find and select the UCH powers that you want.
- 2 Right-click one of the selected UCH powers and select **Delegate Roles and Powers**.
- 3 Search for the specific user, group, or assistant administrator group that you want to delegate powers to.
- 4 Use the **Object Selector** to find and add the objects that you want, and then click **Roles and Powers** in the **Wizard**.
- 5 Click **ActiveViews**, and use the **Object Selector** to find and add the ActiveViews that you want.
- 6 Click **Next** and then **Finish** to complete the delegation process.

Configuring Unified Change History Servers

To configure Unified Change History Servers:

- 1 Log in to the Delegation and Configuration Console.
- 2 Expand **Configuration Management > Integration Servers**.
- 3 Right-click **Unified Change History**, and select **New Unified Change History Server**.
- 4 Specify the UCH server name or IP address, port number, server type, and access account details in the Unified Change History configuration.
- 5 Test the server connection and click **Finish** to save the configuration.
- 6 Add additional servers as required.

Certificate Validation

To enhance security, DRA validates the communication between DRA server and CG server using the CG server certificate. To achieve this, provide details of the certificate bound to the CG server by modifying the 'CGAuditDriver.dll' configuration file present in C:\Program Files (x86)\NetIQ\DRA\X64 and the content need to added as per the below example.

example:

```
<?xml version="1.0" encoding="utf-8"?
<configuration>
<CertificateValidation>
<Certificate server="10.204.102.188" hash="0E982C1D4463590DF4FF1D9626724AE8CBED49B5"/>
<CertificateValidation>
</configuration>
```

To configure multiple CG servers, add multiple entries to the configuration file.

Where,

Certificate server: IP address or host name of the CG server.

Hash: Certificate hash that is bound to the CG server.

By default, audit config file will not be present and operations will continue to work with bypassing certificates.

Restart IIS and DRA Audit Service after adding config file.

Access Unified Change History Reports

To generate and view Unified Change History reports on Active Directory objects via Change Guardian, see [“Generating Change History Reports”](#) in the *Directory and Resource Administrator User Guide*.

Configuring DRA Services for a Group Managed Service Account

If required, you can use a group Managed Service Account (gMSA) for DRA services. For more information about using a gMSA, see the Microsoft reference [Group Managed Service Accounts Overview](#). This section explains how to configure DRA for a gMSA after adding the account to Active Directory.

IMPORTANT: Do not use the gMSA as a service account while installing DRA.

To configure the DRA Primary Administration server for a gMSA:

- 1 Add the gMSA as a member of the following groups:
 - ◆ Local Administrators group on the DRA server
 - ◆ AD LDS group in the DRA managed domain
- 2 Change the logon account in service Properties for each of the services below to the gMSA:
 - ◆ Administration Service
 - ◆ DRA Audit Service
 - ◆ DRA Cache Service
 - ◆ DRA Core Service
 - ◆ DRA Log Archive
 - ◆ DRA Replication Service
 - ◆ DRA Rest Service
 - ◆ DRA Skype Service
- 3 Restart all the services.
- 4 Delegate the “Audit all objects” role to the gMSA by running the following command:

```
Add-DRAAssignments -Identifier "All Objects" -Users "CN=<gMSA_name>, CN=Managed Service Accounts, DC=MyDomain, DC=corp" -Roles "Audit All Objects"
```

To configure a DRA secondary administration server for a gMSA:

- 1 Install the secondary server.
- 2 On the primary server, assign the **Configure Servers and Domains** role to the **Administration Servers and Managed Domains** ActiveView for the secondary server's service account.
- 3 On the primary server, add a new secondary server and specify the secondary server service account.
- 4 Add the gMSA to the local administrators group on the DRA Secondary Administration server.
- 5 On the secondary server, change the logon account of all the DRA services to the gMSA and then re-start the DRA services.

Configure the Delegation and Configuration Client

The Delegation and Configuration client provides access to configuration and delegation tasks, addressing enterprise management needs from distributed administration to policy enforcement. Through the Delegation and Configuration Console, you can set up the security model and server configurations you need to effectively manage your enterprise.

To configure the Delegation and Configuration Client:

- 1 Launch the Delegation and Configuration client, and navigate to **Configuration Management > Update Administration Server Options**.
- 2 Click the **Client Options** tab and define your preferred settings from the configuration options shown:
 - ◆ Allow users to search by ActiveView
 - ◆ Hide source-only objects from console lists
 - ◆ Show advanced Active Directory objects
 - ◆ Show Security command
 - ◆ Show resource and shared mailboxes when searching for users
 - ◆ Default user UPN suffix to current domain
 - ◆ Maximum items editable at a time (Multi-select)
 - ◆ Search Options
 - ◆ Carriage Return Option
 - ◆ Exchange Mailbox Storage Limits Units

Configuring the Web Client

You can configure the Web Console to authenticate using smart cards or multi-factor authentication and also customize the branding with your logo and application title.

- ◆ [“Starting the Web Console” on page 113](#)
- ◆ [“Auto Logout” on page 113](#)
- ◆ [“DRA Server Connection” on page 113](#)

- ◆ “Certificate Validation” on page 114
- ◆ “Authentication” on page 114

Starting the Web Console

You can start the Web Console from any computer, iOS device, or Android device running a Web browser. To start the Console, specify the appropriate URL in your Web browser address field. For example, if you installed the Web component on the HOUserver computer, type `https://HOUserver/draclient` in the address field of your Web browser.

NOTE: To display the most current account and Microsoft Exchange information in the Web Console, set your Web browser to check for newer versions of cached pages at every visit.

Auto Logout

You can define a time increment for the Web Console to log out automatically after inactivity or set it to never log out automatically.

To configure Auto Logout in the Web Console, navigate to **Administration > Configuration > Auto Logout**.

DRA Server Connection

You can use one of the following options to log in to the Web Console. The behavior for each option, when logging in, is described in the following table:

Login Screen - Options	Connection Option Descriptions
Use automatic discovery	Finds a DRA server automatically; no configuration options are available
Connect to the default DRA server	The pre-configured server and port details are used. NOTE: This option is displayed only when you have configured the default DRA server in the Web Console. Also, if you specify that the client must always connect to the default DRA server, you can view only the Connect to the default DRA server option on the login screen.
Connect to a specific DRA server	The user configures the server and port
Connect to a DRA server that manages a specific domain	The user provides a managed domain and chooses a connection option: <ul style="list-style-type: none"> ◆ Use automatic discovery (in the domain provided) ◆ Primary server for this domain ◆ Search for a DRA server (in the domain provided)

To configure the DRA Server connection in the Web Console, navigate to **Administration > Configuration > DRA Server Connection**.

Certificate Validation

To enhance security, DRA validates the communication between client and REST service using the REST service certificate. To achieve this, provide details of the certificate bound to the REST service in the 'restproxy.config' file located under the 'programdata' directory.

For Example:

```
</configuration>  
  
<Certificate server="vlab012723.dom012700.lab"  
hash="7325CCF5ED3A723AC26933BD7F40201C96759D72"/>  
  
</CertificateValidation>
```

Here certificate server can be IP address or hostname of CG server. Hash is the value of the certificate hash that is bound to the REST service.

To configure multiple CG servers, add multiple entries to the configuration file.

Restart IIS service after configuring these changes in the config files.

Authentication

This section contains information for configuring Smart Card Authentication, Windows Authentication, and multi-factor authentication using Advanced Authentication integration.

- ◆ [“Smart Card Authentication” on page 114](#)
- ◆ [“Windows Authentication” on page 116](#)
- ◆ [“Multi-factor Authentication with Advanced Authentication” on page 116](#)

Smart Card Authentication

To configure the Web Console to accept a user based on the client credentials from his or her smart card you must configure Internet Information Services (IIS) and the REST services configuration file.

IMPORTANT: Make sure the certificates on the smart card are also installed in the root certificate store on the web server because IIS must be able to find certificates that match those that are on the card.

- 1 Install authentication components on the web server.
 - 1a Start the Server Manager.
 - 1b Click **Web Server (IIS)**.
 - 1c Go to the Role Services section and click **Add Role Services**.
 - 1d Go to the Security role services node and select **Windows Authentication** and **Client Certificate Mapping Authentication**.
- 2 Enable authentication on the web server.
 - 2a Start **IIS Manager**.
 - 2b Select your web server.

- 2c Find the **Authentication** icon under the IIS section and double-click it.
- 2d Enable “Active Directory Client Certificate Authentication” and “Windows Authentication”.
- 3 Configure the DRA client.
 - 3a Select your DRA client.
 - 3b Find the **Authentication** icon under the IIS section and double-click it.
 - 3c Enable “Windows Authentication” and disable “Anonymous Authentication”.
- 4 Enable SSL and client certificates on the DRA client.
 - 4a Find the **SSL Services** icon under the IIS section and double-click it.
 - 4b Select **Require SSL** and select **Require** under Client certificates.

TIP: If the option is available, select **Require 128-bit SSL**.

- 5 Configure the REST services web application.
 - 5a Select your REST services web application.
 - 5b Find the **Authentication** icon under the IIS section and double-click it.
 - 5c Enable “Windows Authentication” and disable “Anonymous Authentication”.
- 6 Enable SSL and client certificates on the REST services web application.
 - 6a Find the **SSL Services** icon under the IIS section and double-click it.
 - 6b Select **Require SSL** and select **Require** under Client certificates.

TIP: If the option is available, select **Require 128-bit SSL**.

- 7 Configure the WCF web service file.
 - 7a Select your REST services web application and switch to Content View.
 - 7b Locate the .svc file and right-click it.
 - 7c Select **Switch to Features View**.
 - 7d Find the **Authentication** icon under the IIS section and double-click it.
 - 7e Enable “Anonymous Authentication” and disable all other authentication methods.
- 8 Edit the REST services configuration file.
 - 8a Use a text editor to open the C:\inetpub\wwwroot\DRAClient\rest\web.config file.
 - 8b Locate the <authentication mode="None" /> line and delete it.
 - 8c Uncomment the lines specified below:

- ◆ Below the <system.serviceModel> line:

```
<services>
  <service name="NetIQ.DRA.DRARestProxy.RestProxy">
    <endpoint address="" binding="webHttpBinding"
bindingConfiguration="webHttpEndpointBinding"
      name="webHttpEndpoint" contract="NetIQ.DRA.DRARestProxy.IRestProxy"
    />
  </service>
</services>
```

- ◆ Below the <serviceDebug includeExceptionDetailInFaults="false"/> line:

```

<serviceAuthorization impersonateCallerForAllOperations="true" />
  <serviceCredentials>
    <clientCertificate>
      <authentication mapClientCertificateToWindowsAccount="true" />
    </clientCertificate>
  </serviceCredentials>

```

- ◆ Above the `<serviceHostingEnvironment multipleSiteBindingsEnabled="true" />` line:

```

<bindings>
  <webHttpBinding>
    <binding name="webHttpEndpointBinding">
      <security mode="Transport">
        <transport clientCredentialType="Certificate" />
      </security>
    </binding>
  </webHttpBinding>
</bindings>

```

- 9 Save the file and restart the IIS server.

Windows Authentication

To enable Windows authentication on the Web Console you must configure Internet Information Services (IIS) and the REST services configuration file.

- 1 Open IIS Manager.
- 2 In the Connections pane, locate the REST Services web application and select it.
- 3 In the right pane, go to the IIS section and double-click **Authentication**.
- 4 Enable **Windows Authentication** and disable all the other authentication methods.
- 5 Once you enable Windows Authentication, the **Providers** option is added to right-click menu and Actions panel on the right side of the manager window. Open the Providers dialog box and move **NTLM** to the top of the list.
- 6 Use a text editor to open the `C:\inetpub\wwwroot\DRAClient\rest\web.config` file and locate the `<authentication mode="None" />` line.
- 7 Change "None" to "Windows" and save the file.
- 8 Restart the IIS server.

Multi-factor Authentication with Advanced Authentication

Advanced Authentication Framework (AAF) is our premier software package that lets you move beyond a simple user name and password to a more secure way of protecting your sensitive information using multi-factor authentication.

Advanced Authentication supports the following communication protocols for security:

- ◆ TLS 1.2 (default setting), TLS 1.1, TLS 1.0
- ◆ SSL 3.0

Multi-factor authentication is a method of computer access control that requires more than one method of authentication from separate categories of credentials to verify a user's identity.

There are three types of authentication categories or factors:

- ♦ *Knowledge*. This category requires you to know a specific piece of information, such as a password or activation code.
- ♦ *Possession*. This category requires you to have an authenticating device such as a smart card or smartphone.
- ♦ *Body*. This category requires you to use a part of your anatomy, such as your fingerprint, as the method of verification.

Each authentication factor contains at least one authentication method. An authentication method is a specific technique that you can use to establish a user's identity, such as by using a fingerprint or requiring a password.

You can consider an authentication process strong if it uses more than one type of authentication method—for instance, if it requires a password and a fingerprint.

Advanced Authentication supports the following authentication methods:

- ♦ LDAP password
- ♦ Remote Authentication Dial-In User Service (RADIUS)
- ♦ Smartphone

TIP: The Smartphone method requires the user to download an iOS or Android app. For more information, see the *Advanced Authentication - Smartphone Applications User Guide*, which is available from the [Documentation Web site](#).

Use the information in the following sections to configure the Web Console to use multi-factor authentication.

IMPORTANT: While some of the steps in the following sections take place inside the Web Console, most of the multi-factor authentication configuration process requires access to the AAF. These procedures assume that you have already installed AAF and have access to AAF's help documentation.

Adding Repositories to Advanced Authentication Framework

The first step in configuring the Web Console is to use multi-factor authentication to add all the Active Directory domains that contain the DRA administrators and assistant administrators managed by DRA to AAF. These domains are called repositories, and they contain the identity attributes of the users and groups that you want to authenticate.

- 1 Log in to the AAF administration portal with an administrator-level username and password.
- 2 Go to the left panel and click **Repositories**.
- 3 Click **Add**.
- 4 Fill out the form.

TIP

- ♦ The **LDAP type** is **AD**.
 - ♦ Type an administrator-level username and password into the corresponding fields.
-

- 5 Click **Add server**.
- 6 Type the LDAP server's IP address in the **Address** field.
- 7 Click **Save**.
- 8 Repeat Steps 3 through 7 for all other AD repositories managed by DRA.
- 9 For each repository listed on the Repositories page, click **Sync now** to synchronize it with the AAF server.

Creating Authentication Chains

An authentication chain contains at least one authentication method. The methods in the chain will be invoked in the order in which they were added to the chain. For a user to be authenticated, the user must pass all methods in the chain. For example, you can create a chain that contains the LDAP Password method and the SMS method. When a user tries to authenticate using this chain she must first authenticate using her LDAP Password after which a text message will be sent to her mobile phone with a one-time password. After she enters the password all the methods in the chain will have been fulfilled and the authentication succeeds. An authentication chain can be assigned to a specific user or group.

To create an authentication chain:

- 1 Log in to the AAF administration portal with an administrator-level username and password.
- 2 Go to the left panel and click **Chains**. The right panel displays a list of the currently available chains.
- 3 Click **Add**.
- 4 Fill out the form. All fields are required.

IMPORTANT

- ♦ Add the methods in the order in which they should be invoked—that is, if you want the user to enter an LDAP password first, add LDAP password to the chain first.
- ♦ Make sure the **Apply if used by endpoint owner** switch is OFF.

-
- 5 Toggle the **Is enabled** switch to ON.
 - 6 Type the names of the roles or groups to be subject to the authentication request into the **Roles & Groups** field.

TIP: If you want the chain to apply to all users type `all users` into the **Roles & Groups** field and select **All Users** from the resulting drop-down list.

Any user or group that you select will be added beneath the **Roles & Groups** field.

- 7 Click **Save**.

Creating Authentication Events

An authentication event is triggered by an application—in this case, the Web Console—that wants to authenticate a user. At least one authentication chain must be assigned to the event so that when the event is triggered, the methods in the chain associated with the event will be invoked to authenticate the user.

An endpoint is a device—such as a computer or a smartphone—that is running the software that triggers the authentication event. DRA will register the endpoint with AAF after you create the event.

You can use the Endpoints whitelist box to restrict access to an event to specific endpoints, or you can allow all endpoints to access the event.

To create an authentication event:

- 1 Log in to the AAF administration portal with an administrator-level username and password.
- 2 Go to the left panel and click **Events**. The right panel displays a list of the currently available events.
- 3 Click **Add**.
- 4 Fill out the form. All fields are required.

IMPORTANT: Make sure the **Is enabled** switch is ON.

- 5 If you want to restrict access to specific endpoints, go to the Endpoints whitelist section and move the targeted endpoints from the *Available* list to the *Used* list.

TIP: If there are no endpoints in the *Used* list, then the event will be available to all endpoints.

Enabling the Web Console

After you configure chains and events you can log into the Web Console as an administrator and enable Advanced Authentication.

Once authentication is enabled, every user will be required to authenticate through AAF before being given access to the Web Console.

IMPORTANT: Before enabling the Web Console you must already be enrolled in the authentication methods that the Web Console will use to authenticate users. See the *Advanced Authentication Framework User Guide* to learn how to enroll in authentication methods.

To enable Advanced Authentication, log in to the Web Console and navigate to **Administration > Configuration > Advanced Authentication**. Select the **Enabled** check box and configure the form according to the instructions provided for each field.

TIP: After you save the configuration, the endpoint will be created in AAF. To view or edit it, log on to the AAF administration portal with an administrator-level username and password and click **Endpoints** on the left pane.

Final Steps

- 1 Log on to the AAF administration portal with an administrator-level username and password and click **Events** on the left pane.
- 2 Edit each of the Web Console events:
 - 2a Open the event for editing.
 - 2b Go to the Endpoints whitelist section and move the endpoint that you created when you configured the Web Console from the **Available** list to the **Used** list. This will ensure that only the Web Console can use these events.
- 3 Click **Save**.

12 Connecting Managed Systems

This section provides information for connecting and configuring managed systems relating to domains and the Microsoft Exchange components that include Public Folder, Exchange, Office 365, and Skype for Business Online.

- ♦ [“Managing Active Directory Domains” on page 121](#)
- ♦ [“Configuring DRA to Run Secure Active Directory” on page 124](#)
- ♦ [“Connecting Public Folders” on page 125](#)
- ♦ [“Enabling Microsoft Exchange” on page 127](#)
- ♦ [“Configuring Azure Tenants” on page 128](#)
- ♦ [“Managing Passwords for Access Accounts” on page 133](#)
- ♦ [“Enable LDAP Override Authentication” on page 135](#)

Managing Active Directory Domains

You can add new managed domains and computers through the Delegation and Configuration client after you install the Administration server. You can also add subtrees and trusted domains, and configure domain and Exchange access accounts for them. To add managed domains and computers, you must have the appropriate powers, such as those included in the built-in Configure Servers and Domains role.

NOTE: After you finish adding managed domains, ensure that the accounts cache refresh schedules for these domains are correct.

- ♦ [“Adding Managed Domains and Computers” on page 121](#)
- ♦ [“Specifying Domain Access Accounts” on page 122](#)
- ♦ [“Specifying Exchange Access Accounts” on page 122](#)
- ♦ [“Adding a Managed Subtree” on page 123](#)
- ♦ [“Adding a Trusted Domain” on page 124](#)

Adding Managed Domains and Computers

To add a managed domain or computer:

- 1 Navigate to **Configuration Management > New Managed Domain**.

- 2 Specify the component you are adding by selecting the applicable radio button and providing the domain or computer name:
 - ◆ **Manage a domain**
 - ◆ If you want to manage the subtree of a domain, see [Adding a Managed Subtree](#).
 - ◆ If you are adding a new domain with secure LDAP enabled on your domain controllers and you want DRA to use SSL to communicate with your domain controllers, select **This domain is configured for LDAP over SSL**. For more information, see [Configuring DRA to Run Secure Active Directory](#).
 - ◆ **Manage a computer**
- Click **Next** after completing the configuration.
- 3 On the **Domain access** tab, specify the account credentials you want DRA to use to access this domain or computer. By default, DRA uses the Administration server service account.
 - 4 Review the summary, and then click **Finish**.
 - 5 To begin managing objects from this domain or computer, refresh the domain configuration.

Specifying Domain Access Accounts

For each managed domain or subtree, you can specify an account to use instead of the Administration server service account to access that domain. This alternative account is called an access account. To configure an access account, you must have the appropriate powers, such as those included in the built-in Configure Servers and Domains role.

To specify an access account for a member server, you must have permission to manage the domain in which the domain member exists. You can only manage domain members if they exist in a managed domain that you can access through the Administration server.

To specify an access account:

- 1 Navigate to **Configuration Management > Managed Domains** node.
- 2 Right-click the domain or subtree for which you want to specify an access account, and click **Properties**.
- 3 On the Domain access account tab, click **Use the following account to access this domain**.
- 4 Specify and confirm the credentials for this account, and click **OK**.

For information on configuring this least privileged account, see [Least Privilege DRA Access Accounts](#).

Specifying Exchange Access Accounts

For each domain in DRA, you can manage Exchange objects using the DRA domain access account or a separate Exchange access account. To configure an Exchange access account, you must have the appropriate powers, such as those included in the built-in Configure Servers and Domains role.

IMPORTANT: Microsoft Server limits the number of concurrent users connected to the WinRM/WinRS session to five and the number of shells per user to five, so ensure that the same user account is limited to five shells for DRA secondary servers.

To specify an Exchange access account:

- 1 Navigate to **Configuration Management** > **Managed Domains** node.
- 2 Right-click the domain or subtree for which you want to specify an access account, and click **Properties**.
- 3 On the Exchange access account tab, click **Use the following account to access all Exchange servers**.
- 4 Specify and confirm the credentials for this account, and click **OK**.

For information on configuring this least privileged account, see [Least Privilege DRA Access Accounts](#).

Adding a Managed Subtree

You can add managed and missing subtrees from specific Microsoft Windows domains after you install the Administration server. To add a managed subtree, you must have the appropriate powers, such as those included in the built-in Configure Servers and Domains role.

For information about supported versions of Microsoft Windows, see [DRA Administration Server and Web Console Requirements](#).

By managing a subtree of a Windows domain, you can use DRA to secure a department or division within a larger corporate domain.

For example, you can specify the Houston subtree in the SOUTHWEST domain, allowing DRA to securely manage only those objects contained in the Houston OU and its child OUs. This flexibility allows you to manage one or more subtrees without requiring administrative permissions for the entire domain.

NOTE

- ◆ To ensure the specified account has permissions to manage this subtree and perform incremental accounts cache refreshes, use the Deleted Objects Utility to verify and delegate the appropriate permissions.
- ◆ After you finish adding managed subtrees, ensure that the accounts cache refresh schedules for the corresponding domains are correct.

To add a managed subtree:

- 1 Navigate to **Configuration Management**. > **New Manage Domain**.
- 2 On the Domain or server tab, click **Manage a domain**, and specify the domain of the subtree you want to manage.
- 3 Specify the domain of the subtree you want to manage.
- 4 Select **Manage a subtree of this domain**, and then click **Next**.
- 5 On the Subtrees tab, click **Add** to specify the subtree you want to manage. You can specify more than one subtree.
- 6 On the Access account tab, specify the account credentials you want DRA to use to access this subtree. By default, DRA uses the Administration server service account.

- 7 Review the summary, and then click **Finish**.
- 8 To begin managing objects from this subtree, refresh the domain configuration.

Adding a Trusted Domain

Trusted domains enable user authentication on managed systems throughout your managed environment. Once you add a trusted domain, you can specify domain and Exchange access accounts, schedule cache refreshes, and take other actions in the domain's properties, the same as a managed domain.

To add a trusted domain:

- 1 In the **Configuration Management > Managed Domains** node, select the managed domain that has an associated trusted domain.
- 2 Click **Trusted domains** in the Details pane. The Details pane must be toggled on in the View menu.
- 3 Right-click the trusted domain, and select **Properties**.
- 4 Uncheck **Ignore this trusted domain**, and apply your changes.

NOTE: Adding a trusted domain will initiate a full accounts cache refresh, but you will be notified of this with a confirmation prompt when you click **Apply**.

Configuring DRA to Run Secure Active Directory

Secure Active Directory is defined by a DRA environment that is configured to run using the LDAPS (LDAP over SSL) protocol to encrypt communications between DRA and Active Directory to provide a more secure environment.

When upgrading to a DRA 10.x version from a 9.x version, LDAPS needs to be enabled after the upgrade to use Secure Active Directory. The Automatic Discovery feature for detecting and connecting to DRA and REST servers also needs to be configured for this feature.

Enable LDAP Over SSL (LDAPS)

If you are upgrading to DRA 10.x from a 9.x version, follow the steps below. If you are configuring DRA for a new installation, see [Adding Managed Domains and Computers](#).

Note: If a domain is managed using LDAP over SSL, it is necessary to import the appropriate certificate.

- 1 Navigate to **Configuration Management > Managed Domains** in the DRA Delegation and Configuration console.
- 2 Right-click the domain and open Properties.
- 3 Enable **This domain is configured for LDAP over SSL** in the General tab, and click **OK**.
- 4 Restart the Administration Service.

NOTE: If you are also configuring Automatic Discovery to use Secure Active Directory, you can wait to restart services after completing that configuration. For more information, see [Configure Automatic Discovery for LDAPS](#).

Configure Automatic Discovery for LDAPS

Automatic Discovery is the mechanism used by the client to automatically connect to the available DRA environment.

To configure DRA for an environment running Secure Active Directory, configure the `ClientSSLAllDomains` registry key:

- 1 Launch the Registry Editor utility.
- 2 Right-click the `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Mission Critical Software\RestExtensions` node.
- 3 Select **New > DWORD (32-bit) Value**.
- 4 Name the new key `ClientSSLAllDomains`.
- 5 Set the registry key value as 1.
- 6 After adding the `ClientSSLAllDomains` registry key, restart the following services:
 - ◆ World Wide Web Publishing Service
 - ◆ DRA Rest Service.

Connecting Public Folders

DRA enables you to manage Microsoft Exchange Public Folders. You can manage some of the properties of Public Folders using DRA by configuring Public Folder forest domains and granting powers to assistant administrators.

IMPORTANT: To manage Public Folder administration, you must first enable Microsoft Exchange support in DRA and have the applicable powers.

- ◆ For information about enabling Microsoft Exchange, see [Enabling Microsoft Exchange](#).
 - ◆ For information about account permissions, see [Least Privilege DRA Access Accounts](#).
-

To configure Exchange Public Folder support:

- 1 Right-click **Managed Public Folder Forests** in the Configuration and Management node, and click **New Public Folder Forest**.
- 2 Click **Forest Domain**, specify the active directory forest where the public folder objects are located, and then click **Next**.
- 3 In **Domain access**, specify the access account.

IMPORTANT: If you are using the Secondary Server, the **Use the Primary Administration Server domain access account** option will be available.

- 4 In **Exchange access**, specify the account that you want DRA to use for secure access to Exchange servers.

IMPORTANT: If you are using the Secondary Server, the **Use the Primary Administration Server Exchange access account** option will be available.

- 5 In **Exchange server**, select the Exchange Server that you want DRA to use for managing public folders.
- 6 In **Summary**, review the account details and Exchange Server details and then click **Finish** to complete the process.

The DRA server runs full accounts cache refresh on the Public Folder. The new Public Folder forest will appear in the console after the cache refresh completes, which might take a few minutes.

NOTE: You can remove a selected public folder forest domain from the **Tasks** or right-click menu.

- ◆ [“Viewing and Modifying Public Folder Domain Properties” on page 126](#)
- ◆ [“Delegating Public Folder Powers” on page 127](#)

Viewing and Modifying Public Folder Domain Properties

To view or modify Public Folder domain properties:

- 1 Click **Managed Public Folder Forests** in the Configuration Management node, to view the public folders.
- 2 Right-click the Public Folder account you want to view, and select **Properties**.
- 3 In **Public Folder Forest** properties, you can perform the following actions:
 - ◆ **General:** View the public folder account details and update the **Exchange Server** field, which is used by the DRA Server to perform Exchange activity on the Public Folder Server.
 - ◆ **Statistics:** View the number of public folders and the number of mail-enabled public folders.
 - ◆ **Incremental Status:** View or update the incremental accounts cache status.
 - ◆ **Incremental schedule:** View the incremental cache refresh schedule and re-schedule a cache refresh.
 - ◆ **Full status:** View the full account cache refresh status.
 - ◆ **Full refresh:** Perform a full account cache refresh immediately.
If the Public Folder cache data is corrupted, perform a **Full refresh**.
 - ◆ **Domain access:** View DRA service account details or override access accounts.
 - ◆ **Exchange access:** View or update secure access to the Exchange servers.

Delegating Public Folder Powers

Use ActiveViews to define powers and manage Public Folder delegation. You can specify rules to add managed objects, choose domains, and assign powers, and then delegate those Public Folder powers to assistant administrators.

To create an ActiveView and delegate Public Folder powers:

- 1 In the **Delegation Management** node, click **ActiveViews**.
- 2 Click **Next** in the **Create ActiveView Wizard**, select the required rule from the **Add** drop-down list, and choose Public Folders as the object type. For example, to create an object matching rule: select **Objects that match a rule**, and choose **Public Folders** as the object type.
- 3 Specify the ActiveView rule you want to add to the Public Folder, and then click **Next**.
- 4 Specify the name for the ActiveView, and then click **Finish**.
- 5 Right-click **ActiveViews** and go to **Delegate Administration > Assistant Admins**, and specify the Admin type from the **Add** drop-down list in the **Wizard**.
- 6 Search for the specific user, group, or assistant administrator group that you want to delegate powers to.
- 7 Use the **Object Selector** to find and add the objects that you want, and then click **Roles and Powers** in the **Wizard**.
- 8 Select **Roles** from the **Add** drop-down list, and then search and add the Public Folder Administration role.
- 9 Select Powers from the **Add** drop-down list, and then find and add any additional powers that you want to assign to your assistant administrators that are not a part of the Public Folder Administration role.
- 10 Click **Next** and then **Finish** to complete the delegation process.

After you complete the delegation of Public Folder powers, authorized users will be able to perform create, read, update, and delete operations on Public Folder properties in configured domains using the Web Console.

Enabling Microsoft Exchange

Enabling Microsoft Exchange allows you to leverage Exchange and Exchange Online features, including [Microsoft Exchange policies](#), integrated mailbox, and mail-enabled object management. You can enable or disable Microsoft Exchange support on each Administration server for Microsoft Exchange Server 2016 and later versions.

To enable Exchange, you need the required privileges, such as those included in the built-in Manage Policies and Automation Triggers role, and your license must support the Exchange product. For more information about Microsoft Exchange requirements, see [Supported Platforms](#).

To enable support for Microsoft Exchange and Exchange Online:

- 1 Navigate to **Policy and Automation Management > Configure Exchange Policies** in the Delegation and Configuration console.
- 2 Select **Enable Exchange Policy**, and click **Apply**.

Configuring Azure Tenants

DRA allows you to manage MFA enabled Azure tenants using certificate authentication. Basic authentication will be deprecated.

With one or more Azure tenants, you can configure DRA to work with Azure Active Directory to manage Azure objects. These objects include users, guest users, contacts, and groups created in Azure and users, contacts, and groups synchronized with the Azure tenant from DRA managed domains.

The DRA Administrator or an assistant administrator with the delegated role “Configure Servers and Domains” can manage Azure tenants. Azure built-in roles are required to manage Azure objects in the Web Console.

Beginning with DRA 10.2.3, managing Azure tasks requires Azure PowerShell modules, Microsoft.Graph, Az.Accounts Module, and Exchange Online. For more information, see [Supported Platforms](#).

If you are using DRA 10.2.2 or earlier, managing Azure tasks requires Azure PowerShell modules, Azure Active Directory, the Az.Accounts Module, and Exchange Online.

You perform the configuration tasks provided below in the Delegation and Configuration Console. Operations on Azure objects are only performed in the Web Console. For more information, see [Managing Azure Objects](#) in the DRA User Guide.

- ◆ [“Configuring Private Cloud” on page 128](#)
- ◆ [“Adding a New Azure Tenant” on page 129](#)
- ◆ [“Uploading a Certificate Manually” on page 130](#)
- ◆ [“Configuring Certificate-Based Authentication for an Azure Application after Upgrading to 10.2 or later” on page 131](#)
- ◆ [“Resetting the Client Secret for an Azure Application” on page 132](#)
- ◆ [“Configuring the Azure Guest User Invitation” on page 133](#)

Configuring Private Cloud

Private cloud configuration is used when DRA connects to Azure tenants.

To use private cloud, modify the <DRA Install location>/X64/Office365SessionConfig-Custom.xml configuration file and update the values for the ExchangeEnvironmentName and Environment parameters in the following sections:

```
<connect-exchangeonline-parameters> <param name="ExchangeEnvironmentName">O365Default</param> </connect-exchangeonline-parameters>.
```

The following are the values for the ExchangeEnvironmentName parameter: O365USGovGCCHigh, O365USGovDoD, O365GermanyCloud, O365China, and O365Default.

```
<connect-msgraph-parameters> <param name="Environment">Global</param> </connect-msgraph-parameters>.
```


The following are the Possible values for MGGraph: USGov, USGovDoD, Germany, China, and Global.

Adding a New Azure Tenant

Azure tenant can be managed using certificate and basic authentication types. For certificate authentication, we need application with list of permissions. for basic authentication, we need an account in Azure Active Directory. For information on Azure tenant access account permissions, see [Least Privilege DRA Access Accounts](#).

To create an Azure application for DRA and to add Fan Azure tenant:

- 1 Navigate to **Configuration Management > Azure Tenants** in the Delegation and Configuration Console.
 - 2 Right-click **Azure Tenants**, and select **New Azure Tenant**. Click **Next**.
 - 3 Create the Azure application and specify the required details in the **Azure Application** tab.
 - 3a Launch a PowerShell session in the DRA Administration server, and navigate to `C:\Program Files (x86)\NetIQ\DRA\SupportingFiles`
 - 3b Execute `.\NewDraAzureApplication.ps1` to load PowerShell.
 - 3c Execute the `New-DRAAzureApplication` cmdlet by specifying the following parameters:
 - ◆ `<name>` - Name of the application from the tenant wizard.

IMPORTANT: Open Text recommends that you use the name specified in the DRA console.

 - ◆ `<environment>` - DRA 10.2.3: Specify an environment, Users can select the environment value based on the cloud configuration. By default the Global environment is selected. Select Global, China, USGov, USGovDoD or Germany depending on the tenant you are using.
 - ◆ `<environment>` (Optional) - DRA 10.2.2 or earlier: Specify AzureCloud, AzureChinaCloud, AzureGermanyCloud, or AzureUSGovernment, depending on the tenant you are using.
 - 3d In the Credentials dialog box, specify the Global Administrator credentials. The Azure Tenant ID, object ID, application ID, and client secret (application password) are generated.

NOTE: Beginning with 10.2.3, DRA uses both Microsoft.Graph and Exchange Online PowerShell modules, and Microsoft Graph API to access the data. In 10.2.2 and earlier, DRA uses both Azure AD and Exchange Online PowerShell modules, and Microsoft Graph API to access the data. The application ID and application secret are used while accessing Microsoft Graph by using Microsoft Graph API.

 - 3e Copy the Tenant ID, object ID, application ID, and client secret into the **Azure Application** tab of the Add New Azure Tenant Wizard, and click **Next**. DRA validates the Azure application.
- 4 In the **Authentication** tab, select an authentication type.

DRA supports certificate-based authentication and basic authentication for DRA 10.2.2 or earlier while using the Azure AD and Exchange Online PowerShell modules.

- ◆ **Certificate-based authentication:** This is the default option. DRA creates a self-signed certificate and associates the certificate with the Azure application. If you do not want to use the self-signed certificate, you can upload your own certificate after managing the tenant. For more information, see [Uploading a Certificate Manually](#).
- ◆ **Basic authentication:** This is the legacy option. DRA uses the user account that you specify to authenticate with Azure Active Directory (This option is not available in a fresh DRA 10.2.3 installation).

Beginning with DRA 10.2.3, DRA supports only certificate-based authentication, while using the Azure AD and Exchange Online PowerShell modules while adding new tenants.

NOTE: It is recommended to switch to certificate-based authentication for enhanced security. Basic authentication will be deprecated. Users can switch to certificate-based authentication using the Delegation and Configuration console.

Click **Next**.

- 5 (Optional) In the **Custom Azure Tenant Source Anchor Attribute** tab, specify the source anchor attribute used to map your Active Directory objects to Azure during synchronization. Click **Next**.
- 6 Click **Finish**.

Adding the Azure tenant might take several minutes. After the tenant is successfully added, DRA performs a full accounts cache refresh for the tenant and then the added tenant displays in the Azure Tenants view pane.

To view the authentication type for the Azure tenant, right-click the tenant and go to **Properties > Authentication**.

To view the certificate information, right-click the tenant and go to **Properties > Certificate Info**.

Uploading a Certificate Manually

If you want to use your own certificate or if the existing custom certificate has expired and you want to specify a new certificate, you can upload the certificate from the Azure tenant properties page. The supported certificate file formats are `.pfx` and `.cer`

IMPORTANT: Ensure that the manual certificate you specify is protected with a strong password.

To upload a certificate:

- 1 Open the Delegation and Configuration Console and navigate to **Configuration Management > Azure Tenants**.
- 2 Right-click the Azure tenant and go to **Properties > Authentication**. Ensure that the **Manual customer certificate** option is selected.
- 3 Select the **Certificate Info** tab.
- 4 Under **New certificate**, click **Browse** to select a certificate file. If you want to specify a `.cer` certificate file, ensure that a certificate with the private key is installed into the personal store of service account user.
- 5 Specify the password for the certificate, if necessary.

6 Apply the changes. The certificate details are updated.

IMPORTANT:

- ◆ If the primary Administration server is configured with the **Basic authentication**, ensure that you manually specify the credentials for **Basic authentication** on secondary Administration servers for the full accounts cache refresh to be successful. The access account must be unique on each Administration server in the MMS set.
 - ◆ If the primary Administration server is configured with the **Manual customer certificate** or **Automatic self-signed certificate** authentication type, the secondary Administration servers display the authentication type as **Automatic self-signed certificate**. To upload your own certificate, you must manually change the authentication type to **Manual customer certificate** on the secondary Administration server. The certificate must be unique on each Administration server in the MMS set.
-

Configuring Certificate-Based Authentication for an Azure Application after Upgrading to 10.2 or later

After you upgrade to DRA 10.2 or later, you can switch from basic authentication to certificate-based authentication and configure the Azure application to use certificate-based authentication.

NOTE: For enhanced security, it is recommended to transition to certificate-based authentication as basic authentication will be deprecated. Users can make this switch using the Delegation and Configuration console.

The Azure application requires additional permissions for certificate-based authentication. To apply the required permissions to the Azure application, you must run the `UpdateDraAzureApplicationPermission.ps1` script.

To set up the Azure application to use certificate-based authentication after you upgrade, perform the following steps:

- 1 Open the Delegation and Configuration Console and navigate to **Configuration Management > Azure Tenants**.
- 2 Right-click the Azure tenant and select **Properties > Authentication**. The **Basic authentication** option is selected by default.
- 3 Change the authentication type to **Automatic self-signed certificate** or **Manual customer certificate**.
- 4 Click the **Certificate Info** tab.
- 5 Update the Azure application by applying the necessary permissions for certificate-based authentication.
 - 5a Launch a PowerShell session in the DRA Administration server, and navigate to `C:\Program Files (x86)\NetIQ\DRA\SupportingFiles`
 - 5b Execute `.\UpdateDraAzureApplicationPermission.ps1` to load PowerShell.
 - 5c Execute the `UpdateDraAzureApplicationPermission` cmdlet by specifying the name of the Azure application that is available in the Azure Application tab.

- 5d In the Credentials dialog box, specify the Global Administrator credentials. The application object ID is generated.
- 5e Copy the application object ID into the **Certificate Info** tab. If you have selected the **Manual customer certificate** option, upload the certificate in the New Certificate area.
- 6 Apply the changes. The certificate details are updated.

Resetting the Client Secret for an Azure Application

Follow the steps below if you need to reset the client secret for an Azure application.

To reset the client secret for an Azure application:

- 1 Launch a PowerShell session in the DRA Administration server and navigate to `C:\Program Files (x86)\NetIQ\DRAsupportingFiles`
- 2 Execute `.\ResetDraAzureApplicationClientSecret.ps1` to load PowerShell.
- 3 Execute the `ResetDraAzureApplicationClientSecret` cmdlet to prompt for parameters.
- 4 Specify the following parameters for `Reset-DraAzureApplicationClientSecret`:
 - ◆ `<name>` - Name of the application from the tenant wizard.
 - ◆ `<environment>` - DRA 10.2.3: Specify an Environment value, users can select the environment value based on their cloud configuration they have, by default the Global environment is selected. Select AGlobal, China, USGov, USGovDoD or Germany depending on the tenant you are using.
 - ◆ `<environment>` (optional) - DRA 10.2.2 or earlier, specify AzureCloud, AzureChinaCloud, AzureGermanyCloud, or AzureUSGovernment, depending on which tenant you are using.
- 5 In the Credentials dialog box, specify the Global Administrator credentials.
The Azure application ID and client secret are generated.
- 6 Copy the client secret into the DRA console (tenant wizard).
 - 6a Open the Delegation and Configuration Console and navigate to **Configuration Management > Azure Tenants**.
 - 6b Right-click the Azure tenant and go to **Properties > Azure Application**.
 - 6c Paste the Azure application client secret that is generated from the script into the **Client Secret** field.
 - 6d Apply the changes.

Configuring the Azure Guest User Invitation

When you invite Azure guest users to Azure Active Directory, DRA sends an email to the Azure guest user with a customized welcome message that includes an invitation link. You can configure this welcome message and the invitation link or redirect URL that you want to be displayed in the invitation. An Azure guest user is redirected to the configured URL after accepting the invitation, where Azure guest users can log in using their credentials.

To configure the guest user invitation:

- 1 Navigate to **Configuration Management** > **Azure Tenants** in the Delegation and Configuration Console.
- 2 Select the managed Azure tenant for which you want to configure the invite, right-click and select **Properties**.
- 3 Click the **Guest Invite Config** tab.
- 4 Specify the welcome message and the invitation link.
- 5 Apply the changes.

Managing Passwords for Access Accounts

You can reset passwords for access accounts that are used to manage a domain, secondary server, Exchange, or Azure tenant from DRA. If the password for any of these access accounts is due to expire or if you forget the password, you can reset the password for the access account in the following ways:

- ♦ Reset the password manually in the Delegation and Configuration Console.
- ♦ Schedule a job to monitor password expiration for access accounts and reset the password for access accounts that are due to expire.

You can reset the password for access accounts from both the primary server and secondary server. If the same access account is used at multiple instances in the same domain, for example, to manage an Exchange mailbox or a secondary server, the DRA server automatically updates the password for all instances of the access account usage, thus eliminating the need for manually updating the password for each instance. If the secondary Administration server uses the domain access account of the primary Administration server, the DRA server automatically refreshes the password for the access account in the secondary Administration server.

- ♦ [“Reset Password Manually” on page 133](#)
- ♦ [“Schedule a Job to Reset Password” on page 134](#)

Reset Password Manually

Use the Delegation and Configuration Console to manually reset the password for an access account.

To manually reset the password for an access account:

- 1 In the Delegation and Configuration console, click **Configuration Management**.
- 2 Select a managed domain or an Azure tenant and view properties.

3 On the properties page, specify the following information:

- ◆ To update the password for a domain access account, in the Domain access tab, specify a new password for the domain access account. Select **Update password in Active Directory**.
- ◆ To update the password for an Exchange access account, in the Exchange access tab, specify a new password for the Exchange access account. Select **Update password in Active Directory**.
- ◆ To update the password for an Azure tenant access account, in the Tenant access tab, specify a new password for the tenant access account. Select **Update Azure tenant access account password**.
- ◆ To update the password for an access account for a secondary Administration server, select **Configuration Management > Administration Servers** in the primary Administration server. Select the secondary Administration server for which you want to update the password, right-click and select **Properties**. In the Access account tab, specify a new password for the access account. Select **Update password in Active Directory**.

NOTE

- ◆ Ensure that the access account of the secondary Administration server is not the service account of the secondary Administration server. The access account must be a part of the Local Administrators group on the secondary Administration server.
 - ◆ If you use the least privilege account as the access account, ensure that the account is assigned the “Reset Password” permission for itself in Active Directory for the password reset to be successful in DRA.
-

Schedule a Job to Reset Password

You can schedule the Reset Password job to run at a predefined interval to reset expiring passwords for your access accounts. The job will reset any access account passwords that are due to expire before the next time the job is scheduled to run. A new password will be automatically generated according to the password policy.

The job is disabled by default. You can schedule the job once a week or at a specific interval, according to your requirement. In an MMS environment, if you configure the job on the primary server, ensure that the job is configured on all servers in the MMS.

To configure the job:

- 1 On the server that you want to schedule the job, go to the registry entry
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Mission Critical
Software\OnePoint\Administration\Modules\Accounts\UpdateAccessAccPWD.F
req.
- 2 Right-click and select **Modify**.
- 3 In the **Value data** field, specify the frequency at which you want the job to run.
 - ◆ To schedule a weekly job, specify the frequency in the format `Weekly <Day of the week> <Time in 24-hour format>`. For example, to schedule the job to run every Saturday at 6.00 PM, enter:
`Weekly 06 18:00`

Where 6 indicates the day of the week and 18:00 indicates the time in the 24-hour format.

- ◆ To schedule the job to run at a specific interval, specify the frequency in the format `Interval <Time in 24-hour format>`. For example, to schedule the job to run every 8 hours, enter:

```
Interval 08:00
```

It is recommended to schedule the job to run on weekends.

NOTE: The Reset Password job does not support daily frequency. If you configure daily frequency, DRA Server automatically resets the schedule to `Weekly 06 00:00` when you restart the DRA Administrative Service.

4 Click **OK**.

5 Restart DRA Administration Service for the changes to take effect.

NOTE: For each Azure tenant configured, the job creates the following registry key for the default password policy with a validity of 90 days:

```
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Mission Critical  
Software\OnePoint\Administration\Modules\Accounts\<tenantName>.ValidityPer  
iod. The password expiry date for the tenant access account is calculated based on the validity  
period for the tenant. When the password is due to expire, the job resets the password for the  
tenant access account.
```

Enable LDAP Override Authentication

You can configure an LDAP override authentication for LDAP custom handler modifications in the Web Console. With this feature enabled, you can set the authentication type for custom LDAP query handlers to require the LDAP Override Account for connection authentication.

To enable this feature:

- 1 Navigate to **Configuration Management > Update Administration Server Options** in the Delegation and Configuration Console.
- 2 Select the **LDAP Override Account** tab in the Administration Server Options window.
- 3 Provide the account name, domain, and password and apply the changes.

For example: `name@domain` or `domain\name`

For information about using this feature in Web Console customizations, see [Basic Steps for Creating a Custom Handler](#).

V Policy and Process Automation

This chapter provides information to help you understand how policies work in the DRA environment and what those policy options are. It also explains how triggers and Automated Workflow are used to automate processes when working with objects in Active Directory.

- ♦ [Chapter 13, “Understanding DRA Policy,” on page 139](#)
- ♦ [Chapter 14, “Pre and Post Task Trigger Automation,” on page 159](#)
- ♦ [Chapter 15, “Automated Workflow,” on page 163](#)

13 Understanding DRA Policy

DRA enables you to configure various policies that help you secure your enterprise and prevent data corruption. These policies work within the context of the dynamic security model, ensuring that policy enforcement automatically keeps up with your changing enterprise. Establishing policies, such as naming conventions, disk usage limits, and property validation allows you to enforce rules that help maintain the integrity of your enterprise data.

In DRA you can quickly define policy rules for these enterprise management areas:

- ◆ Microsoft Exchange
- ◆ Office 365 License
- ◆ Home Directory
- ◆ Password generation

DRA also supplies built-in policies for groups, user accounts, and computers.

To manage or define policies, you must have the appropriate powers, such as those included in either the DRA Admins or Manage Policies and Automation Triggers roles. To help you manage your policies, DRA provides the Policy Details report. This report provides the following information:

- ◆ Indicates whether the policy is enabled
- ◆ Lists associated operations
- ◆ Lists objects governed by this policy
- ◆ Provides policy scope details

You can use this report to ensure that your policies are defined properly. You can also use this report to compare policy properties, identify conflicts, and enforce better policies across your enterprise.

How the Administration Server Enforces Policy

You can associate each task, or administration operation, with one or more policies. When you perform an operation associated with a policy, the Administration server runs the policy and enforces the specified rules. If the server detects a policy violation, it returns an error message. If the server does not detect a policy violation, it completes the operation. You can limit the scope of a policy by associating it with a particular ActiveView or Assistant Admin group.

If an operation is associated with more than one policy, the Administration server enforces the policies in alphabetical order. That is, Policy A will be enforced before Policy B, regardless of the specified rules.

To ensure that your policies do not conflict with each other, use the following guidelines:

- ◆ Name the policies so that they execute in the proper order
- ◆ Verify that each policy does not interfere with validations or actions performed by other policies
- ◆ Thoroughly test custom policies before implementing them in your production environment

The Administration server enters the policy status in the audit log each time a policy runs. These log entries record the return code, associated operations, objects acted on, and whether the custom policy succeeded.

WARNING: Policies are run using the Administration service account. Since the service account has administrator permissions, policies have full access to all enterprise data. Thus, assistant administrators associated with the built-in Manage Policies and Automation Triggers role could obtain more power than you intended.

Built-in Policy

Built-in policies are implemented when you install the Administration server. When you work with these policies, you may encounter the following terms:

Policy scope

Defines the objects or properties to which DRA applies the policy. For example, some policies allow you to apply a policy to specific assistant administrators in specific ActiveViews. Some policies let you choose from different classes of objects, such as user accounts or groups.

Global policies

Enforce policy rules on all objects of the specified class or type in the managed domains. Global policies do not let you limit the scope of the objects to which the policy applies.

Policy relationship

Defines whether the policy applies jointly or by itself. To establish a policy relationship, define two or more rules that apply to the same action, and choose the member of a policy group option. If the operation parameters or property matches any of the rules, the operation succeeds.

Built-in policy topics:

- ♦ [“Understanding Built-in Policies” on page 141](#)
- ♦ [“Available Policies” on page 141](#)
- ♦ [“Using Built-in Policy” on page 143](#)

Understanding Built-in Policies

Built-in policies provide business rules to address common security and data integrity issues. These policies are part of the default security model, allowing you to integrate DRA security features into your existing enterprise configuration.

DRA provides two ways to enforce a policy. You can create custom policies or choose from several built-in policies. Built-in policies make it easy to apply policy without having to develop custom scripts. If you need to implement a custom policy, you can adapt an existing built-in policy to fit your needs. Most policies allow you to modify the error message text, rename the policy, add a description, and specify how to apply the policy.

A number of built-in policies are enabled when you install DRA. The following policies are implemented by default. If you do not want to enforce these policies, you can disable them or delete them.

Policy Name	Default Value	Description
\$ComputerNameLengthPolicy	64 15 (pre-Windows 2000)	Limits the number of characters in the computer name or the pre-Windows 2000 computer name
\$GroupNameLengthPolicy	64 20 (pre-Windows 2000)	Limits the number of characters in the group name or the pre-Windows 2000 group name
\$GroupSizePolicy	5000	Limits the number of members in a group
\$NameUniquenessPolicy	None	Ensures pre-Windows 2000 and CN names are unique in all managed domains
\$SpecialGroupsPolicy	None	Prevents unchecked escalation of powers in the environment.
\$UCPowerConflictPolicy	None	Prevents escalation of power by making User Clone and User Create powers mutually exclusive
\$UPNUniquenessPolicy	None	Ensures UPN names are unique in all managed domains
\$UserNameLengthPolicy	64 20 (down-level logon name)	Limits the number of characters in the user logon name or the down-level logon name

Available Policies

DRA provides several policies you can customize for your security model.

NOTE: You can create a policy that requires an entry for a property that is not currently available from the DRA user interfaces. If an entry is required by policy and the user interface does not provide a field to enter the value, such as a department for new user account, you will not be able to create or manage the object. To avoid this issue, configure policies that require only those properties that can be accessed from the user interfaces.

Create a Custom Policy

Allows you to link a script or executable to a DRA or Exchange operation. Custom policies let you validate any operations you choose.

Enforce a Maximum Name Length

Allows you to globally enforce maximum name length for user accounts, groups, OUs, contacts, or computers.

The policy checks the name container (common name, or `cn`) and the pre-Windows 2000 name (user logon name).

Enforce Maximum Number of Group Members

Allows you to globally enforce limits on the number of members in a group.

Enforce Unique Pre-Windows 2000 Account Names

Verifies that a pre-Windows 2000 name is unique across all managed domains. In Microsoft Windows domains, pre-Windows 2000 names must be unique within a domain. This global policy enforces this rule across all managed domains.

Enforce unique User Principal Names (UPNs)

Verifies that a user principal name (UPN) is unique across all managed domains. In Microsoft Windows domains, UPNs must be unique within a domain. This policy enforces this rule across all managed domains. Because this is a global policy, DRA provides the policy name, description, and policy relationship.

Limit actions on members of special groups

Prevents you from managing members of an administrator group unless you are a member of that administrator group. This global policy is enabled by default.

When you limit actions on members of the administrator groups, the Create Policy Wizard does not require additional information. You can specify a custom error message. Because this is a global policy, DRA provides the policy name, description, and policy relationship.

Prevent assistant administrators from Creating and Cloning Users in Same AV

Prevents possible escalation of powers. When this policy is enabled, you can either create user accounts or clone user accounts, but you cannot have both powers. This global policy ensures that you cannot create and clone user accounts in the same ActiveView.

This policy does not require additional information.

Set Naming Convention Policy

Allows you to establish naming conventions that apply to specific assistant administrators, ActiveViews, and classes of objects, such as user accounts or groups.

You can also specify the exact names monitored by this policy.

Create a Policy to Validate a Specific Property

Allows you to create a policy to validate any property of an OU or an account object. You can specify a default value, a property format mask, and valid values and ranges.

Use this policy to enforce data integrity by validating a particular entry field when you create, clone, or modify properties of specific objects. This policy provides tremendous flexibility and power to validate entries, provide default entries, and limit entry choices for various property fields. By using this policy, you can require that a correct entry be made before the task is completed, thereby maintaining data integrity across your managed domains.

For example, assume you have three departments: Manufacturing, Sales, and Administration. You can limit the entries DRA will accept to just these three values. You can also use this policy to enforce proper telephone number formats, supply a range of valid data, or require an entry

for the email address field. To specify multiple format masks for a telephone number, such as (123) 456 7890 as well as 456 7890, define the property format mask as (###)### ####,### #####.

Create Policy to Enforce Office 365 Licenses

Allows you to create a policy to assign Office 365 licenses based on Active Directory group membership. This policy also enforces the removal of Office 365 licenses when a member is removed from the relevant Active Directory group.

If a user who is not synchronized to the cloud is added to the Active Directory group, the user will be synchronized before an Office 365 license is assigned to the user.

During the creation of the policy, you can specify several properties and settings, such as the name of the policy and the wording of the error message that appears when an assistant administrator attempts an action that violates this policy.

The **Ensure only licenses assigned by DRA policies are enabled on accounts. All other licenses will be removed.** setting is included in the Tenant Properties page, which is configurable per tenant. This setting is used for DRA Office 365 license policies to configure how license assignments will be enforced:

When this setting is enabled, the DRA license enforcement will ensure that only licenses assigned through DRA policies are provisioned to accounts (licenses assigned outside of DRA will be removed from the accounts assigned to the license policy). When this setting is disabled (default), DRA license enforcement will only ensure that the specific licenses you have included in your Office 365 policies are provisioned to accounts (when an account is unassigned from a license policy, only the licenses assigned by that policy will be de-provisioned).

Using Built-in Policy

Because built-in policy is part of the default security model, you can use these policies to enforce your current security model or modify them to better meet your needs. You can change the name, rule settings, scope, policy relationship, and error message of several built-in policies. You can enable or disable each built-in policy.

You can also easily create new policies.

Implementing a Custom Policy

Custom policies allow you to fully exploit the power and flexibility of the default security model. By using custom policies, you can integrate DRA with existing enterprise components while ensuring that your proprietary rules are enforced. You can use the custom policy feature to extend your enterprise policies.

You create and enforce custom policies by associating an executable or a script to an administration operation. For example, a policy script associated with the `UserCreate` operation could check your human resource database to see if the specified employee exists. If the employee exists in the human resources database and does not have an existing account, the script retrieves the employee ID, first name, and last name from the database. The operation completes successfully and populates the user account property window with the proper information. However, if the employee already has an account, the operation fails.

Scripts give you a tremendous amount of flexibility and power. To create your own policy scripts, you can use the Directory and Resource Administrator ADSI Provider (ADSI provider), Software Development Kit (SDK), and PowerShell cmdlets. For more information about creating your own policy scripts, see the Reference section on the [DRA Documentation](#) site.

Restricting Native Built-in Security Groups

To provide a more secure environment, DRA allows you to limit the powers given to Microsoft Windows built-in security groups. The ability to modify group membership, built-in security group properties, or properties of the group members can have important security implications. For example, if you can change the password of a user in the Server Operators group, you can then log on as that user and exercise the powers delegated to this built-in security group.

DRA prevents this security issue by providing a policy that checks the powers you have for a native built-in security group and its members. This validation ensures that your requested actions do not escalate these powers. After you enable this policy, an assistant administrator who is a member of a built-in security group, such as the Server Operators group, can only manage other members of the same group.

Native Built-in Security Groups You Can Restrict

You can restrict the powers of the following Microsoft Windows built-in security groups using DRA policies:

- ◆ Account Operators
- ◆ Administrators
- ◆ Backup Operators
- ◆ Cert Publishers
- ◆ DNS Admins
- ◆ Domain Admins
- ◆ Enterprise Admins
- ◆ Group Policy Creator Owners
- ◆ Print Operators
- ◆ Schema Admins

NOTE: DRA refers to the built-in security groups by their internal identifiers. As a result, DRA supports these groups even if the groups are renamed. This feature ensures that DRA supports built-in security groups with different names in different countries. For example, DRA refers to the Administrators group and the *Administratoren* group with the same internal identifier.

Restricting Actions on Native Built-in Security Groups

DRA uses policy to limit the power native built-in security groups and their members can exercise. This policy, called `$SpecialGroupsPolicy`, restricts the actions a member of a native built-in security group can perform on other members or other native built-in security groups. DRA enables this policy by default. If you do not want to restrict actions on native built-in security groups and their members, you can disable this policy.

When this policy is enabled, DRA uses the following validation tests to determine whether an action is permitted on a native built-in security group or its members:

- ◆ If you are a Microsoft Windows administrator, you can perform actions on native built-in security groups and their members for which you have the appropriate powers.
- ◆ If you are a member of a built-in security group, you can perform actions on the same built-in security group and its members, if you have the appropriate powers.
- ◆ If you are not a member of a built-in security group, you cannot modify a built-in security group or its members.

For example, if you are a member of the Server Operators and Account Operators groups and you have the appropriate powers, you can perform actions on members of the Server Operators group, members of the Account Operators group, or members of both groups. However, you cannot perform actions on a user account that is a member of the Print Operators group and the Account Operators group.

DRA restricts you from performing the following actions on native built-in security groups:

- ◆ Cloning a group
- ◆ Creating a group
- ◆ Deleting a group
- ◆ Adding a member to a group
- ◆ Removing a member from a group
- ◆ Moving a group to an OU
- ◆ Modifying properties of a group
- ◆ Copying a mailbox
- ◆ Removing a mailbox
- ◆ Cloning a user account
- ◆ Creating a user account
- ◆ Deleting a user account
- ◆ Moving a user account to an OU
- ◆ Modifying user account properties

DRA also restricts actions to ensure you do not gain powers over an object. For example, when you add a user account to a group, DRA checks to ensure you do not gain additional powers over the user account because it is a member of that group. This validation helps protect against an escalation of power.

Managing Policies

Through the Policy and Automation Management node, you can access Microsoft Exchange and home directory policies, as well as built-in and custom policies. Use the following common tasks to improve your enterprise security and data integrity.

Configure Exchange Policies

Enables you to define Microsoft Exchange configuration, mailbox policy, automatic naming, and proxy generation rules. These rules can define how mailboxes are managed when an assistant administrator creates, modifies, or deletes a user account.

Configure Home Directory Policies

Enables you to automatically create, rename, or delete home directories and home shares when an assistant administrator creates, renames, or deletes a user account. The Home directory policy also allows you to enable or disable disk quota support for home directories on Microsoft Windows servers as well as on non-Windows servers.

Configure Password Generation Policies

Enables you to define the requirements for passwords generated by DRA.

For more detailed information about managing policies in DRA, reference the following sections:

- ♦ [“Microsoft Exchange Policy” on page 146](#)
- ♦ [“Office 365 License Policy” on page 148](#)
- ♦ [“Creating and Implementing Home Directory Policy” on page 149](#)
- ♦ [“Enabling Password Generation” on page 155](#)
- ♦ [“Policy Tasks” on page 155](#)

Microsoft Exchange Policy

These policies can help you streamline your workflows and maintain data integrity. For example, you can specify how Exchange manages mailboxes when you create, modify, or delete user accounts. To define and manage Microsoft Exchange policies, you must have the appropriate powers, such as those included in the built-in Manage Policies and Automation Triggers role.

Configuring a Default Email Address Policy

To specify default email address policy, you must have the appropriate powers, such as those included in the built-in Manage Policies and Automation Triggers role, and your license must support the Exchange product.

To specify a default email address policy:

- 1 Navigate to **Policy and Automation Management > Configure Exchange Policies > Proxy Generation**.

- 2 Specify the domain of the Microsoft Exchange server.
 - 2a Click **Browse**.
 - 2b Specify additional search criteria as needed, and then click **Find Now**.
 - 2c Select the domain to configure, and then click **OK**.
- 3 Specify the proxy generation rules for the selected domain.
 - 3a Click **Add**.
 - 3b Select a proxy type. For example, click **Internet Address**.
 - 3c Accept the default value or type a new proxy generation rule, and then click **OK**.
For more information about supported substitution strings for proxy generation rules, see [Delegation and Configuration Client Policy](#)
- 4 Click **Custom attributes** to edit the custom name of custom mailbox properties.
 - 4a Select the attribute and click the **Edit** button.
 - 4b In the Attribute Properties window, enter the attribute name in the **Custom name** field, and click **OK**.
- 5 Click **OK**.

NOTE: DRA Policy Admins should have the *Manage Custom Tools* power to modify custom attributes in the Microsoft Exchange policy.

Configuring a Remote Routing Address Policy

A remote address routing policy allows you to specify a rule to generate a remote routing address. The client uses this policy to generate a remote routing address while creating a remote mailbox.

To specify a default remote routing address policy:

- 1 Navigate to **Policy and Automation Management > Configure Exchange Policies > Remote routing address generation**.
- 2 Select a hybrid domain from the **Select the hybrid domain to view and update the remote routing address generation rule** list.
- 3 Specify the rule to generate the remote routing address.
 - 3a Click **Custom**.
 - 3b Select an address type from the **Remote routing address type** list. For example, click **Internet Address**.
 - 3c Type a rule definition in the **Remote routing address generation** field.
You can use the following substitution strings in the rule definition: `%First`, `%Last`, `%Initials`, `%Alias`, and `%UserName`
 - 3d Select a UPN suffix.
 - 3e Click **Apply**.
- 4 Click **OK**.
To delete the rule for the domain, select **None**.

Mailbox Rules

Mailbox rules let you specify how Exchange manages mailboxes when assistant administrators create, clone, modify, or delete user accounts. Mailbox rules automatically manage Microsoft Exchange mailboxes based on how the assistant administrator manages the associated user accounts.

NOTE: When enabling the **Do not allow Assistant Admins to create a user account without a mailbox** option in Microsoft Windows domains, ensure that the assistant administrator has the power to either clone or create a user account. Enabling this option requires assistant administrators to create Windows user accounts with a mailbox.

To specify Microsoft Exchange mailbox rules, you must have the appropriate powers, such as those included in the built-in Manage Policies and Automation Triggers role, and your license must support the Exchange product.

To specify Exchange mailbox rules:

- 1 Navigate to **Policy and Automation Management > Configure Exchange Policies > Mailbox Rules**.
- 2 Select the mailbox policies you want Exchange to enforce when you create or modify user accounts.
- 3 Click **OK**.

Office 365 License Policy

To specify Office 365 license policies, you must have the appropriate powers, such as those included in the built-in Manage Policies and Automation Triggers role. Your license must also support the Microsoft Exchange product.

Allowing DRA to Manage your Office 365 Licenses (Optional)

If you want to allow DRA to manage your Office 365 licenses, you must do the following:

- ♦ Create a license enforcement policy.
- ♦ Enable the **License update schedule** on the tenant properties page.

Creating a Policy to Enforce Office 365 Licenses

To create a policy to enforce Office 365 licenses, navigate to **Policy and Automation Management > Policy** in the Delegation and Configuration console, and select **New Policy > Create New Policy to Enforce Office 365 Licenses**.

When the policy is enforced and a user is added to Active Directory, DRA uses group membership to automatically assign the Office 365 license to the user.

Office 365 License Update Schedule

Policies that you create to enforce Office 365 licenses are not applied when changes are made outside of DRA unless you also enable the **License update schedule** on the tenant properties page. The license update job ensures that the Office 365 licenses assigned to users match your Office 365 license policies.

The license update job and Office 365 license policies work together to ensure that all your managed users are assigned only the Office 365 licenses they are supposed to have.

NOTE

- ◆ DRA does not manage Office 365 licenses for online-only user accounts. For DRA to manage your users with Office 365 licenses, those users must be synchronized with Active Directory.
 - ◆ If you choose to use DRA to manage your Office 365 licenses, DRA will override any manual changes to Office 365 licenses made outside of DRA the next time the license update job runs.
 - ◆ If you enable the Office 365 license update job before ensuring that your Office 365 license policies are configured properly, your assigned licenses might be incorrect after the license update job runs.
-

Creating and Implementing Home Directory Policy

When you manage a large number of user accounts, creating and maintaining these home directories and shares can require a lot of time and can be a source of security errors. Additional maintenance can be required each time a user is created, renamed, or deleted. Home directory policies help you manage home directory and home share maintenance.

DRA allows you to automate the creation and maintenance of user home directories. For example, you can easily configure DRA so that the Administration server creates a home directory when you create a user account. In this case, if you specify a home directory path when you create the user account, the server automatically creates the home directory per the specified path. If you do not specify a path, the server does not create the home directory.

DRA supports Distributed File System (DFS) paths during creation of user home directories or configuration of home directory policies for users in allowable parent paths. You can create, rename, and delete home directories on Netapp Filers and DFS paths or partitions.

Configuring Home Directory Policies

To configure home directory, share, and volume disk quota policies, you must have the appropriate powers, such as those included in the built-in Manage Policies and Automation Triggers role. Each policy automatically manages home directories, share, and volume disk quota based on how you manage the associated user accounts.

To configure home directory policies, navigate to **Policy and Automation Management > Configure Home Directory Policies**. Select the appropriate home directory options and configure.

- ◆ Home directory
- ◆ Home share
- ◆ Home Volume Disk Quota

Administration Server Requirements

For each computer where you need to create a home share, the Administration server service account or access account should be an administrator on that computer or a member of the Administrators group in the corresponding domain.

An administration share, such as C\$ or D\$, must exist for each drive on which DRA manages and stores home directories. DRA uses the administration shares to perform some home directory and home share automation tasks. If these shares do not exist, DRA cannot provide home directory and home share automation.

Configuring Home Directory Allowable Paths for NetApp Filers

To configure the Allowable Parent Paths for a NetApp Filer:

- 1 Navigate to **Policy and Automation Management > Configure Home Directory Policies**.
- 2 In the **Allowable parent paths** text box, enter one of the allowable paths from the following table:

Share type	Allowable path
Windows	(\\ <i>FileName</i> \adminshare:\volumerootpath\directorypath)
Non-Windows	(\\ <i>non-windows</i> \share)

- 3 Click **Add**.
- 4 Repeat Steps 1-3 for each allowable parent path wherever you want to apply the home directory policies.

Understanding Home Directory Policy

To be consistent with proper Microsoft Windows security policies, DRA creates access control restrictions at the directory level only. Placing access control restrictions at both the share name level and the file or directory object level often leads to a confusing access scheme for administrators and users.

When you change an access control restriction for a home share, DRA does not change the existing security for that directory. In this case, you must ensure that the user accounts have the appropriate access to their own home directories.

Home Directory Automation and Rules

DRA automates home directory maintenance tasks by managing home directories when you modify a user account. DRA can perform different actions when a user account is created, cloned, modified, renamed, or deleted.

To successfully implement your home directory policy, consider the following guidelines:

- ◆ Ensure the specified path uses the correct format.
 - ◆ To specify a path for a single home directory, use one of the templates from the following table:

Share Type	Path Template
Windows	<code>\\computer\share\.</code> For example, if you want DRA to automatically create a home directory in the Home Share folder on the server01 computer, type <code>\\server01\Home Share\</code>
Non-Windows	<code>\\non-windows\share</code>

- ◆ To standardize home directory administration on the root directory of the corresponding home share, use the Universal Naming Convention syntax, such as `\\server name\C:\path to root directory`.
- ◆ To specify a path for nested home directories, use one of the templates from the following table:

Share Type	Path Template
Windows	<code>\\computer\share\first directory\second directory\</code> For example, if you want DRA to automatically create a home directory in the existing JSmith\Home directory under the Home Share folder on the server01 computer, type <code>\\server01\Home Share\JSmith\Home</code> .
Non-Windows	<code>\\non-windows\share\first directory\second directory\</code>

NOTE: DRA also supports the following formats: `\\computer\share\username` and `\\computer\share\%username%`. In each case, DRA automatically creates a home directory for the associated user account.

- ◆ When you define a policy or automation trigger for managing home directories on a NetApp filer, you need to use a different format for the directory specification.
 - ◆ If you are using NetApp filers, specify the parent directory in the following format:
`\\FilerName\adminshare:\volumerootpath\directorypath`
 - ◆ The adminshare variable is the hidden share that maps to the root volume on the NetApp filer, such as c\$. For example, if the local path of the share on a NetApp filer, called usfiler, is c\$\vol\vol10\mydirectory, you can specify a root path of
`\\usfiler\c:\vol\vol10\mydirectory` for the NetApp filer.
- ◆ To specify a DFS path while you create user home directories or configure home directory policies for users, use `\\server\root\<link>` format, where root can be either the managed domain or a standalone root directory in the following format:
`\\FilerName\adminshare:\volumerootpath\directorypath`.
- ◆ Create a shared directory to store the home directory for this user account.
- ◆ Ensure that DRA can access the computer or share referenced in the path.

Create home directory when user account is created

This rule allows DRA to automatically create home directories for new user accounts. When DRA creates a home directory, the Administration server uses the path specified in the **Home directory** fields in the Create User Wizard. You can later modify this path through the Profile tab of the user properties window and DRA will move the home directory to the new location. If you do not specify values for these fields, DRA does not create a home directory for that user account.

DRA sets the security for the new directory based on the selected **Home directory permissions** options. These options let you control the general access for all home directories.

For example, you can specify that members of the Administrators group have full control and members of the Help Desk group have read access to the share in which the user home directories are created. Then, when DRA creates a user home directory, the new home directory can inherit these rights from the parent directory. Therefore, members of the Administrators group have Full Control over all user home directories and members of the Help Desk group have read access to all user home directories.

If the specified home directory already exists, DRA does not create the home directory and does not modify the existing directory permissions.

Rename home directory when user account is renamed

This rule allows DRA to automatically perform the following actions:

- ◆ Create a home directory when you specify a new home directory path
- ◆ Move home directory contents when you change the home directory path
- ◆ Rename a home directory when you rename the user account

When you rename a user account, DRA renames the existing home directory based on the new account name. If the existing home directory is currently in use, DRA creates a new home directory with the new name and does not change the existing home directory.

When you change the home directory path, DRA attempts to create the specified home directory and move the contents of the previous home directory to the new location. You can also configure the Home Directory policy to create a home directory without moving the contents from the existing home directory. DRA also applies the assigned ACLs from the

previous directory to the new directory. If the specified home directory already exists, DRA does not create this new directory and does not modify the existing directory permissions. If the previous home directory is not locked, DRA deletes it.

When DRA fails to rename the home directory, DRA tries to create a new home directory with a new name and copy the contents from the previous home directory to the new home directory. DRA then attempts to delete the previous home directory. You can configure DRA not to copy the contents from the previous home directory to the new home directory and manually move the contents from the previous home directory to the new home directory to avoid concerns such as copying open files.

While deleting the previous home directory, DRA requires explicit permission to delete read-only files and subdirectories from the previous home directory. You can provide DRA the permission to explicitly delete the read-only files and subdirectories from the previous home directory.

Allow parent directory or path for a home share

DRA allows you to specify the allowable parent directories or paths for home shares on file servers. If you have many directory or file server paths to specify, you can export these paths to a CSV file and add the paths from the CSV file to DRA using the DRA console. DRA uses the information entered in the **Allowable parent paths** field to ensure:

- ◆ DRA does not delete the parent directory on the file server when assistant administrators delete a user account and the user account home directory.
- ◆ DRA moves the home directory to a valid parent directory or path on the file server when you rename a user account or change the home directory path for a user account.

Delete home directory when user account is deleted

This rule allows DRA to automatically delete a home directory when you delete the associated user account. If you enable the Recycle Bin, DRA does not delete the home directory until you delete the user account from the Recycle Bin. While deleting the home directory, DRA requires explicit permission to delete read-only files and subdirectories from the previous home directory. You can provide DRA the permission to explicitly delete the read-only files and subdirectories from the previous home directory.

Home Share Automation and Rules

DRA automates home share maintenance tasks by managing home shares when you modify a user account or manage home directories. DRA can perform different actions when a user account is created, cloned, modified, renamed, or deleted.

To be consistent with proper Microsoft Windows security policies, DRA does not create access control restrictions at the share name level. Instead, DRA creates access control restrictions at the directory level only. Placing access control restrictions at both the share name level and the file or directory object level often leads to a confusing access scheme for administrators and users.

NOTE: The specified location must have a common home share, such as `HOMEDIRS`, at one level above the home directories.

For example, the following path is valid: `\\HOUSERV1\HOMEDIRS\%username%`

The following path is invalid: `\\HOUSERV1\%username%`

Specifying Home Share Names

When defining the home share automation rules, you can specify a prefix and suffix for each automatically created home share. By specifying a prefix or suffix, you can enforce a naming convention for home shares.

For example, you enable the Create home directory and Create home share automation rules. For the home share, you specify an underscore prefix and a dollar sign suffix. When you create a user named TomS, you map his new directory to the U drive and specify `\\HOUSERV1\HOMEDIRS\%username%` as the directory path. In this example, DRA creates a network share named `_TomS$` that points to the `\\HOUSERV1\HOMEDIRS\TomS` directory.

Creating Home Shares for New User Accounts

When DRA creates a home share, the Administration server uses the path specified in the **Home directory** fields in the Create User Wizard. You can later modify this path through the Profile tab of the user properties window.

DRA creates the share name by adding the specified prefix and suffix, if any, to the user name. If you use long user account names, DRA may not be able to add the specified home share prefix and suffix. The prefix and suffix, as well as the number of permitted connections, are based on the home share creation options you select.

Creating Home Shares for Cloned User Accounts

If the home share name generated from the newly created user account name already exists, DRA deletes the existing share and create a new share to the specified home directory.

When cloning a user account, the share name of the existing user account must currently exist. When you clone a user account, DRA also clones the home directory information and customizes that information for the new user.

Modifying Home Share Properties

When you change the home directory location, DRA deletes the existing share and creates a new share to the new home directory. If the original home directory is empty, DRA deletes the original directory.

Renaming Home Shares for Renamed User Accounts

When you rename a user account, DRA deletes the existing home share and creates a new share based on the new account name. The new share points to the existing home directory.

Deleting Home Shares for Deleted User Accounts

When you permanently delete a user account, DRA deletes the home share.

Home Volume Disk Quota Management Rules

DRA allows you to manage disk quotas for home volumes. You can implement this policy in native domains where the home directory resides on a Microsoft Windows computer. When you implement this policy, you should specify a disk quota of at least 25MB, to allow for ample room.

Enabling Password Generation

This feature enables you to specify the policy settings for passwords that DRA generates. DRA does not enforce these settings on passwords that users create. When configuring Password Policy properties, the password length must be no less than 6 characters and no more than 127 characters, all the values can be set to zero except for the password length and maximum limit.

To configure Password Generation Policies, navigate to **Policy and Automation Management > Configure Password Generation Policies**, and select the **Enable Password Policy** check box. Click **Password Settings** and configure the Password Policy properties.

Policy Tasks

To delete, enable, or disable policies, you must have the appropriate powers, such as those included in the built-in Manage Policies and Automation Triggers role.

To perform one of these actions, navigate to **Policy and Automation Management > Policy**. Right-click the policy that you want to delete, enable, or disable in the right pane, and select the desired action.

Implementing Built-in Policies

To implement built-in policies, you must have the appropriate powers, such as those included in the built-in Manage Policies and Automation Triggers role. For more information about built-in policies, see [Understanding Built-in Policies](#).

NOTE: Before associating the built-in policy with an assistant administrator and an ActiveView, first verify that the assistant administrator is assigned to that ActiveView.

To implement built-in policies:

- 1 Navigate to **Policy and Automation Management > Policy**.
- 2 On the Tasks menu, click **New Policy**, and then select the type of built-in policy you want to create.
- 3 On each wizard window, specify the appropriate values, and then click **Next**. For example, you can associate this new policy with a specific ActiveView, allowing DRA to enforce this policy on objects included by that ActiveView.
- 4 Review the summary, and then click **Finish**.

Implementing Custom Policies

To implement a custom policy, you must have the appropriate powers, such as those included in the built-in Manage Policies and Automation Triggers role.

To successfully implement a custom policy, you must write a script that runs during a specific operation (administrative task). You can associate an executable or a script to the operation. DRA supports both 32-bit PowerShell script and 64-bit PowerShell script. In the custom policy script, you can define error messages to display whenever an action violates the policy. You can also specify a default error message through the Create Policy Wizard.

For more information about writing custom policies, viewing a list of Administration operations, or using argument arrays, see the SDK. For more information, see [Writing Custom Policy Scripts or Executables](#).

NOTE

- ◆ Before associating the custom policy with an assistant administrator and an ActiveView, first ensure that the assistant administrator is assigned to that ActiveView.
 - ◆ If the path of the custom policy script or executable contains spaces, specify quotation marks (") around the path.
-

To implement a custom policy:

- 1 Write a policy script or executable.
- 2 Log on to a DRA client computer with an account that is assigned the built-in Manage Policies and Automation Triggers role in the managed domain.
- 3 Start the Delegation and Configuration console.
- 4 Connect to the primary Administration server.
- 5 In the left pane, expand **Policy and Automation Management**.
- 6 Click **Policy**.
- 7 On the Tasks menu, click **New Policy > Create a Custom Policy**.
- 8 On each wizard window, specify the appropriate values, and then click **Next**. For example, you can associate this new policy with a specific ActiveView, allowing DRA to enforce this policy on objects included by that ActiveView.
- 9 Review the summary, and then click **Finish**.

Modifying Policy Properties

To modify all the properties of a policy, you must have the appropriate powers, such as those included in the built-in Manage Policies and Automation Triggers role.

To modify policy properties:

- 1 Navigate to **Policy and Automation Management > Policy**.
- 2 Right-click the policy you want to modify, and select **Properties**.
- 3 Modify the appropriate properties and settings for this policy.

Writing Custom Policy Scripts or Executables

For more information about writing a custom policy scripts or executables, see the SDK.

To access the SDK:

- 1 Ensure that you have installed the SDK on your computer. The setup program creates a shortcut to the SDK in the Directory and Resource Administrator program group. For more information, see the installation checklist at [Install the DRA Administration Server](#).
- 2 Click the SDK shortcut in the Directory and Resource Administrator program group.

Delegation and Configuration Client Policy

Automatic naming policy includes three policy configurations in Exchange Policies that are exclusive to the Delegation and Configuration client, meaning it is a client-side policy.

Automatic naming policy allows you to specify automated naming rules for specific properties of a mailbox. These options allow you to establish naming conventions and quickly generate standard values for the display name, directory name, and alias properties. Exchange allows you to specify substitution strings, such as `%First` and `%Last`, for several automated naming options.

When Exchange generates a directory name or alias, it checks whether the generated value is unique. If the generated value is not unique, Exchange appends a hyphen (-) and a two-digit number, starting with `-01`, to make the value unique. When Exchange generates a display name, it does not check whether the value is unique.

Exchange supports the following substitution strings for automatic naming and proxy generation policies:

%First	Indicates the value of the First name property for the associated user account.
%Last	Indicates the value of the Last name property for the associated user account.
%Initials	Indicates the value of the Initials property for the associated user account.
%Alias	Indicates the value of the Alias mailbox property.
%DirName	Indicates the value of the Directory name mailbox property. When generating email addresses for Microsoft Exchange mailboxes, Exchange does not support proxy generation strings that specify the <code>%DirName</code> variable.
%UserName	Indicates the value of the User name property for the associated user account.

You can also specify a number between the percent sign (%) and the substitution string name to indicate the number of characters to include from that value. For example, `%2First` indicates the first two characters from the **First** name property of the user account.

Each automatic naming rule, proxy generation policy, or remote routing address generation policy can contain one or more substitution strings. You can also specify characters in each rule as a prefix or suffix for a specific substitution string, such as a period and space (.) following the `%Initials` substitution string. If the property for the substitution string is blank, the Exchange does not include the suffix for that property.

For example, consider the following auto naming rule for the **Display** name property:

```
%First %1Initials. %Last
```

If the **First** name property is Susan, the **Initials** property is May, and the **Last** name property is Smith, Exchange sets the **Display** name property to Susan M. Smith.

If the **First** name property is Michael, the **Initials** property is blank, and the **Last** name property is Jones, Exchange sets the **Display** name property to Michael Jones.

Specifying an Automated Mailbox Naming Policy

To specify automated mailbox naming options, you must have the appropriate powers, such as those included in the built-in Manage Policies and Automation Triggers role, and your license must support the Exchange product.

To specify an automated mailbox naming policy:

- 1 Navigate to **Policy and Automation Management > Configure Exchange Policies > Alias naming**.
- 2 Specify the appropriate name generation information.
- 3 Select **Enforce alias naming rules during mailbox updates**.
- 4 Click **OK**.

Specifying a Resource Naming Policy

To specify resource naming options, you must have the appropriate powers, such as those included in the built-in Manage Policies and Automation Triggers role, and your license must support the Exchange product.

To specify a resource naming policy:

- 1 Navigate to **Policy and Automation Management > Configure Exchange Policies > Resource naming**.
- 2 Specify the appropriate resource name generation information.
- 3 Select **Enforce resource naming rules during mailbox updates**.
- 4 Click **OK**.

Specifying an Archive Naming Policy

To specify archive naming options, you must have the appropriate powers, such as those included in the built-in Manage Policies and Automation Triggers role, and your license must support the Exchange product.

To specify an archive naming policy:

- 1 Navigate to **Policy and Automation Management > Configure Exchange Policies > Archive naming**.
- 2 Specify the appropriate archive name generation information for user accounts.
- 3 Select **Enforce archive naming rules during mailbox updates**.
- 4 Click **OK**.

14 Pre and Post Task Trigger Automation

An automation trigger is a rule that associates a script or executable file with one or more operations. Through the script or executable file, you can automate an existing workflow and establish an information bridge between DRA and other data repositories. Automation triggers allow you to extend the functionality and security that DRA offers.

When you define an automation trigger, you set the rule parameters, which operations should be associated with the trigger, which script or executable to run, and, if applicable, which ActiveViews or assistant administrators should be associated with this trigger. These rules determine how the Administration server applies your trigger.

You can also specify an undo script or executable for your trigger. An **undo script** allows you to rollback your changes if the operation fails.

DRA supports VBscript and PowerShell scripts.

How the Administration Server Automates Processes

In addition to ActiveView rules based administration, DRA enables you to automate your existing workflows and automatically run related tasks through automation triggers. Automating existing workflows can help you streamline your enterprise while providing better and faster services.

When the Administration server runs the operation associated with your automation trigger, the server also runs the trigger script or executable. If your trigger is a pre task trigger, the server runs the script or executable before running the operation. If your trigger is a post task trigger, the server runs the script or executable after running the operation. This process is called a transaction. A **transaction** represents the full implementation cycle for each task, or operation, the Administration server performs. A transaction includes the actions required to complete an operation along with any undo actions the Administration server should perform if the operation fails.

The Administration server enters the trigger status in the Audit log each time an automation trigger runs. These log entries record the return code, associated operations, objects acted on, and whether the trigger script succeeded.

WARNING: Automation triggers are run using the Administration server service account. Since the service account has administrator permissions, policies and automation triggers have full access to all enterprise data. To define automation triggers, you must have the appropriate powers, such as those included in the built-in Manage Policies and Automation Triggers role. These automation triggers will run within the service account security context. Thus, assistant administrators associated with the built-in Manage Policies and Automation Triggers role could obtain more power than you intended.

Implementing an Automation Trigger

To implement automation triggers, you must first write trigger scripts or executables and have the appropriate powers, such as those included in the built-in Manage Policies and Automation Triggers role.

To successfully implement a custom trigger, you must write a script that runs during a specific operation (administrative task). You can associate an executable or a script to the operation. DRA supports both 32-bit PowerShell script and 64-bit PowerShell script. You can specify whether DRA applies the trigger before (pre-task) or after (post-task) an operation runs. In the trigger script, you can define error messages to display whenever the trigger fails. You can also specify a default error message through the Create Automation Trigger Wizard.

For more information about writing custom triggers, viewing a list of Administration operations, or using argument arrays, see the *SDK*.

NOTE

- ◆ Before associating the custom automation trigger with an assistant administrator and an ActiveView, first ensure that the assistant administrator is assigned to that ActiveView.
- ◆ If the path of the custom trigger script or executable contains spaces, specify quotation marks (") around the path.
- ◆ Currently, if the **UserSetInfo** operation is used for a script automation trigger and a user attribute is changed (executing the trigger), the changed attribute is not proliferated across the enterprise until after a **Find Now** operation is run on the user object.

To implement an automation trigger:

- 1 Write a trigger script or executable file.
- 2 Log on to a DRA client computer with an account that is assigned the built-in **Manage Policies and Automation Triggers** role in the managed domain.
- 3 Start the Delegation and Configuration console.
- 4 Connect to a primary Administration server.
- 5 Use **File Replication** to upload the trigger file to the DRA primary and secondary servers.
The folder path must already exist on all DRA servers in the managed domain. This path, including the file, will be used in the **Do file path** of the Automation Trigger wizard.
- 6 In the left pane, expand **Policy and Automation Management**.
- 7 Click **Automation Triggers**.
- 8 On the Tasks menu, click **New Trigger**.
- 9 On each wizard window, specify the appropriate values, and then click **Next**. For example, you can associate this new trigger with a specific ActiveView, allowing DRA to apply this trigger when assistant administrators manage objects included by that ActiveView.
- 10 Review the summary, and then click **Finish**.

IMPORTANT: If you have more than one ActiveView configured for a trigger by adding a comma between ActiveViews, those ActiveViews get bifurcated in the trigger when upgrading to a new version of DRA and the trigger will not execute. For the operation to execute after upgrade, the trigger will need to be reconfigured or a new trigger will need to be created.

15 Automated Workflow

Using Workflow Automation you can automate IT processes by creating customized workflow forms that run on execution of a workflow or when triggered by a named workflow event that is created in the Workflow Automation server. When you create a workflow form, you define the Admin groups that can view the form. Form submission or workflow process execution is dependent on the powers delegated to the group or groups included when creating the workflow form.

Workflow forms, when created or modified, are saved to the Web Server. Assistant administrators logging onto the Web Console for this server will have access to the forms based on how you configure the form. Forms are generally available to all users with web server credentials. You limit access to a specific form by adding Assistant Admin groups and then hiding the form from other users. The capability to submit the form requires one of the following powers:

- ◆ Create Workflow Event and Modify All Properties
- ◆ Start Workflow

Launching a workflow form: Workflows are created in the Workflow Automation Server, which must be integrated with DRA through the Delegation and Configuration Console. To save a new form, you must have either the **Launch Specific Workflow** or **Trigger Workflow by Event** option configured in the form properties. More information about these options is provided below:

- ◆ **Launch Specific Workflow:** This option lists all the available workflows that are in production in the Workflow Server for DRA. For the workflows to populate in this list, they need to be created in the `DRA_Workflows` folder in the Workflow Automation server.
- ◆ **Trigger Workflow by Event:** This option is used to execute workflows with pre-defined triggers. The workflows with triggers are also created in the Workflow Automation server.

NOTE: Only workflow requests configured with Launch Specific Workflow will have an execution history that can be queried in the main search pane under **Tasks > Requests**.

You can modify an existing request or create a new request. To modify an existing request, navigate to **Tasks > Requests**.

To create a workflow request, navigate to **Administration > Customization > Requests**.

To create a request, follow these basic steps:

1. Configure the request to execute a *specified workflow* when the form is submitted, or configure the request to execute when triggered by a predefined *named event*.
2. Choose the Assistant Admin group or groups that are included in the workflow process, and enable the **Form is hidden** option in the **General** tab to restrict form access to these users.
3. Add any required property fields or additional property pages to the form.
4. If applicable, create custom handlers to further define the workflow process and how it executes.

NOTE: Custom handler options are not exposed for a new workflow request until the request is initially saved. You can access, create, and modify custom handlers in **Form Properties**.

5. Disable the **Form is hidden** option to enable users to view forms.

For information about configuring the Workflow Automation server, see [Configuring the Workflow Automation Server](#) and for customizing workflow requests, see [Customizing Request Forms](#).

VI Auditing and Reporting

Auditing user actions is among the most important aspects of a sound security implementation. To allow you to review and report on assistant administrator actions, DRA logs all user operations in the log archive on the Administration server computer. DRA provides clear and comprehensive reporting that includes before and after values of the audited events so that you can see exactly what changed.

- ♦ [Chapter 16, “Auditing Activity,” on page 167](#)
- ♦ [Chapter 17, “Reporting,” on page 173](#)

16 Auditing Activity

Auditing activity in event logs can help you isolate, diagnose, and resolve issues in your environment. This section provides information to help you enable and understand event logging and how to work with log archives.

Native Windows Event Log

To allow you to review and report on assistant administrator actions, DRA logs all user operations in the log archive on the Administration server computer. User operations include all attempts to change definitions, such as updating user accounts, deleting groups, or redefining ActiveViews. DRA also logs specific internal operations, such as Administration server initialization and related server information. In addition to logging these audit events, DRA logs the before and after values for the event so that you can see exactly what changed.

DRA uses a folder, **NetIQLogArchiveData**, called a **log archive** to securely store archived log data. DRA archives the logs over time and then deletes older data to make room for newer data through a process called grooming.

DRA uses the audit events stored in the log archive files to display Activity Detail reports, such as showing what changes have been made to an object during a specified time. You can also configure DRA to export information from these log archive files to a SQL Server database that Reporting Center uses to display Management reports.

DRA always writes audit events to the log archive. You can enable or disable having DRA write events to the Windows event logs as well.

Enabling and Disabling Windows Event Log Auditing for DRA

When you install DRA, audit events are not logged in the Windows event log by default. You can enable this type of logging by modifying a registry key.

WARNING: Be careful when editing your Windows Registry. If there is an error in your Registry, your computer may become nonfunctional. If an error occurs, you can restore the Registry to its state when you last successfully started your computer. For more information, see the Help for the Windows Registry Editor.

To enable event auditing:

- 1 Click **Start > Run**.
- 2 Type `regedit` in the **Open** field and click **OK**.
- 3 Expand the following registry key: `HKLM\Software\WOW6432Node\Mission Critical Software\OnePoint\Administration\Modules\ServerConfiguration\`.
- 4 Click **Edit > New > DWORD Value**.
- 5 Enter `IsNTAuditEnabled` as the key name.

- 6 Click **Edit > Modify**.
- 7 Enter 1 in the **Value data** field and click **OK**.
- 8 Close Registry Editor.

To disable event auditing:

- 1 Click **Start > Run**.
- 2 Type `regedit` in the **Open** field and click **OK**.
- 3 Expand the following registry key: `HKLM\Software\WOW6432Node\Mission Critical Software\OnePoint\Administration\Modules\ServerConfiguration\`.
- 4 Select the `IsNTAuditEnabled` key.
- 5 Click **Edit > Modify**.
- 6 Enter 0 in the **Value data** field and click **OK**.
- 7 Close Registry Editor.

Ensuring Auditing Integrity

To ensure that all user actions are audited, DRA provides alternate logging methods when the product cannot verify logging activity. When you install DRA, the `AuditFailsFilePath` key and path are added to your registry to ensure the following actions:

- ◆ If DRA detects that audit events are no longer being logged in a log archive, DRA logs the audit events in a local file on the Administration server.
- ◆ If DRA cannot write audit events to a local file, DRA writes audit events to the Windows event log.
- ◆ If DRA cannot write audit events to the Windows event log, the product writes audit events to the DRA log.
- ◆ If DRA detects that audit events are not being logged, it blocks further user operations.

To enable write operations when the log archive is unavailable, you must also set a registry key value for the `AllowOperationsOnAuditFailure` key.

WARNING: Be careful when editing your Windows Registry. If there is an error in your Registry, your computer may become nonfunctional. If an error occurs, you can restore the Registry to its state when you last successfully started your computer. For more information, see the Help for the Windows Registry Editor.

To enable write operations:

- 1 Click **Start > Run**.
- 2 Type `regedit` in the **Open** field and click **OK**.
- 3 Expand the following registry key: `HKLM\Software\WOW6432Node\Mission Critical Software\OnePoint\Administration\Audit\`.
- 4 Click **Edit > New > DWORD Value**.
- 5 Enter `AllowOperationsOnAuditFailure` as the key name.
- 6 Click **Edit > Modify**.

- 7 Enter 736458265 in the **Value data** field.
- 8 Select **Decimal** in the **Base** field and click **OK**.
- 9 Close Registry Editor.

Understanding Log Archives

DRA logs user activity data in log archives on the Administration server. DRA creates daily log archive partitions to store data collected and normalized that day. DRA uses the date in the local time on the Administration server (YYYYMMDD) as the naming convention for daily log archive partitions.

If you have enabled the Management Reports Collector, DRA exports log archive data to a SQL Server database as the source for DRA Management reports.

Initially, DRA retains log data in the log archive indefinitely by default. The log archive size can reach a maximum size that is determined at installation time based on available hard drive space. When the log archive exceeds this maximum size, no new audit events are stored. You can set a time limit for data retention, and DRA removes the oldest data to make room for newer data through a process called grooming. Ensure you have a backup strategy in place before you enable grooming. You can configure the log archive retention period using the Log Archive Configuration utility. For more information, see [Modifying Log Archive Grooming Settings](#).

Using the Log Archive Viewer Utility

You use the Log Archive Viewer utility to view data stored in log archive files. The DRA Log Archive Resource Kit (LARK), which you can choose to install with DRA, provides the Log Archive Viewer utility. For more information, see the [DRA Log Archive Resource Kit Technical Reference](#).

Backing up Log Archive Files

A **log archive file** is a collection of record blocks. Because log archive files are compressed binary files that are located outside of a physical database, you do not need to use Microsoft SQL Server Management Studio to back up log archives. If you have an automated file backup system in place, your log archive files are backed up automatically like any other file.

Keep in mind the following best practices when planning your backup strategy:

- ♦ A single partition is created each day that contains event data for that day. When you enable grooming, the Log Archive Service will groom the data from these partitions automatically every 90 days by default. The backup strategy should consider the grooming schedule to determine the frequency of the backups. When the log archive partitions are groomed, DRA deletes the binary files. You cannot retrieve groomed data. You must restore groomed data from a backup. For more information, see [Modifying Log Archive Grooming Settings](#).
- ♦ You should only back up partitions after they have been closed. Under normal conditions, a partition is closed within 2 hours of midnight the next day.
- ♦ Back up and restore partition folders and all their subfolders as a unit. Backup the `VolumeInfo.xml` file as part of the partition backup.

- ♦ If you want to restore log archive partitions for reports, ensure backed up log archives retain or can be restored to their original format.
- ♦ When configuring your process for backing up log archive files, exclude both the `index_data` and `CubeExport` subfolders located in the main log archive folder. These subfolders contain temporary data and should not be backed up.

Modifying Log Archive Grooming Settings

When you install DRA, log archive grooming is disabled by default. When you establish regular backup procedures for your log archive files, you should enable log archive grooming to conserve disk space. You modify the number of days before log archive partitions are groomed using the Log Archive Configuration utility.

To change the number of days before log archive partitions are groomed:

- 1 Log on to the Administration server using an account that is a member of the Local Administrators group.
- 2 Start **Log Archive Configuration** in the Administration program group.
- 3 Click **Log Archive Server Settings**.
- 4 *If you want to enable partition grooming*, set the value of the **Partition Grooming Enabled** field to True.
- 5 Type the number of days you want to retain log archive partitions before grooming in the **Number of Days before Grooming** field.
- 6 Click **Apply**.
- 7 Click **Yes**.
- 8 Click **Close**.
- 9 Locate the path to the `NetIQLogArchiveData\<Partition Name>` folder, typically:

`C:\ProgramData\NetIQ\DRA\NetIQLogArchiveData`

If the “File is ready for archiving” attribute on the files or folders within the specified partitions is not checked (in the file or folder properties), you must edit the CONFIG file to enable log archive grooming. To understand why this attribute might or might not be checked, see the **Additional Information** section in the Knowledgebase article [How do you configure the data retention period for DRA Logarchival Data?](#).

If value is

Checked

Click **Yes** on the confirmation message to restart the Security Manager Log Archive service.

NOTE: If you modify any log archive setting, you must restart the Log Archive service for the change to take effect.

Not checked

Click **No** on the confirmation message. See [To enable the DRA Log Archive Server to groom unarchived data:](#).

To enable the DRA Log Archive Server to groom unarchived data:

- 1 Log on locally to each DRA server windows console as a member of the local administrators group.
- 2 Use a text editor to open the `C:\ProgramData\NetIQ\Directory Resource Administrator\LogArchiveConfiguration.config` file and locate the `<Property name="GroomUnarchivedData" value="false" />` line.
- 3 Change "false" to "true" and save the file.
- 4 Restart the DRA LogArchive Service.

NOTE: If you modify any log archive setting, you must restart the Log Archive service for the change to take effect.

17 Reporting

This section provides information for understanding and enabling DRA reporting, reporting data collection, ActiveView Analyzer collection and reporting, and accessing built-in reports.

DRA disables functions and reports that your license does not support. You must also have the appropriate powers to run and view reports. Therefore, you may not have access to some reports.

Activity Detail reports are available in Delegation and Configuration console as soon as you install DRA to provide the latest details on your network changes.

- ◆ [“Managing Data Collection for Reporting” on page 173](#)
- ◆ [“Built-in Reports” on page 174](#)

Managing Data Collection for Reporting

DRA Reporting provides two methods of generating reports that allow you to see the latest changes in your environment and to collect and review user account, group, and resource definitions in your domain.

Activity Detail reports

Accessed through the Delegation and Configuration console, these reports provide real-time change information for objects in your domain.

DRA Management reports

Accessed through Reporting Center, these reports provide activity, configuration, and summarization information about events in your managed domains. Some reports are available as graphical representations of the data.

For example, you can view a list of changes made to an object or by an object during a specified time period using Activity Detail reports. You can also view a graph showing the number of events in each managed domain during a specified time period using Management reports. Reporting also allows you to view details about the DRA security model, such as ActiveView and assistant administrator group definitions.

DRA Management reports can be installed and configured as an optional feature and are viewed in Reporting Center. When you enable and configure data collection, DRA collects information about audited events and exports it to a SQL Server database on a schedule that you define. When you connect to this database in Reporting Center, you have access to over 60 built-in reports:

- ◆ Activity reports that show who did what, and when
- ◆ Configuration reports that show the state of AD or DRA at a specific point in time
- ◆ Summarization reports that show activity volume

For more information about configuring data collection for Management reports, see [Reporting Configuration](#).

Viewing the Collectors Status

You can view details of each data collector on the Collectors Status tab.

To view the status of the collectors:

- 1 Expand **Configuration Management**, and then click **Update Reporting Service Configuration**.
- 2 On the Collectors Status tab, click each entry to view additional information about data collection, such as when data was last collected and whether the last data collection was successful.
- 3 If you see no data in the Server list, click **Refresh**.

Enabling Reporting and Data Collection

After installing DRA Reporting components, enable and configure reporting data collection to access Reporting Center reports.

To enable reporting and data collection:

- 1 Navigate to **Configuration Management > Update Reporting Service Configuration**.
- 2 On the SQL Server tab, select **Enable DRA Reporting support**.
- 3 Click **Browse** in the Server Name field and select the computer where SQL Server is installed.
- 4 On the Credentials tab, specify the appropriate credentials to use for the SQL Server interactions.
- 5 If this is the same account that can be used to create the database and initialize the schema, select the Use the above credentials for creating a database and initializing the database schema check box.
- 6 If you want to specify a different account for creating a database, on the Admin Credentials tab, specify that user account and password.
- 7 Click **OK**.

For information on configuring specific collectors, see [Reporting Configuration](#).

Built-in Reports

Built-in reports give you the capability to generate reports on object changes, object lists, and object details. These reports are not part of DRA Reporting Services and no configuration is required to enable built-in change history reports. Reference the topics in this section to learn how to access these reports.

NOTE: Change history reports can also be accessed for events outside of DRA when DRA is integrated with Change Guardian. For information on these types of reports and configuring a Change Guardian server, see [“Configure Unified Change History” on page 109](#).

Reporting on Object Changes

You can view real-time change information for objects in your domains by generating Activity Detail reports. For example, you can view a list of changes made to an object or by an object during a specified time period. You can also export and print Activity Detail reports.

To report on object changes:

- 1 Find the objects that match your criteria.
- 2 Right-click an object, and select **Reporting > Changes made to objectName** or **Reporting > Changes made by objectName**.
- 3 Select the start and end dates to specify the changes you want to view.
- 4 *If you want to change the number of rows to be displayed, type a number over the default value of 250.*

NOTE: The number of rows displayed applies to each Administration server in your environment. If you include 3 Administration servers in the report and use the default value of 250 rows to display, up to 750 rows can be displayed in the report.

- 5 *If you want to include only specific Administration servers in the report, select **Restrict query to these DRA servers** and type the server name or names you want the report to include. Separate multiple server names with commas.*
- 6 Click **OK**.

Reporting on Object Lists

You can export or print data from object lists. With this feature, you can quickly and easily report on and distribute general information about your managed objects.

When you export an object list, you can specify the file location, name, and format. DRA supports HTML, CSV, and XML formats, so you can export this information to database applications or post list results to a Web page

NOTE: You can also select multiple items in a list and then copy these items to a text application, such as Notepad.

To report on object lists:

- 1 Find the objects that match your criteria.
- 2 To export this object list, click **Export List** on the File menu.
- 3 To print this object list, click **Print List** on the File menu.
- 4 Specify the appropriate information to save or print this list.

Reporting on Object Details

You can export or print data from details tabs that list object attributes, such as group memberships. With this feature, you can quickly and easily report on and distribute frequently needed details about specific objects.

When you export an object details tab, you can specify the file location, name, and format. DRA supports HTML, CSV, and XML formats, so you can export this information to database applications or post list results to a Web page.

To report on object details:

- 1 Find the object that matches your criteria.
- 2 On the View menu, click **Details**.
- 3 In the details pane, select the appropriate tab.
- 4 To export these object details, click **Export Details List** on the File menu.
- 5 To print these object details, click **Print Details List** on the File menu.
- 6 Specify the appropriate information to save or print this list.

VII Additional Features

Temporary Group Assignments, Dynamic Groups, Event Stamping, and BitLocker Recovery Password are additional features in DRA that you can employ in your enterprise environment.

- ♦ [Chapter 18, “Temporary Group Assignments,” on page 179](#)
- ♦ [Chapter 19, “DRA Dynamic Groups,” on page 181](#)
- ♦ [Chapter 20, “How Event Stamping Works,” on page 183](#)
- ♦ [Chapter 21, “BitLocker Recovery Password,” on page 185](#)
- ♦ [Chapter 22, “Recycle Bin,” on page 187](#)

18 Temporary Group Assignments

The Manage Temporary Group Assignments role grants assistant administrators the powers to create and manage temporary group assignments.

Assistant administrators can only view temporary group assignments for groups that the assistant administrator has powers to add or remove members from.

Use the following powers to delegate the creation and management of temporary group assignments:

- ◆ Create Temporary Group Assignments
- ◆ Delete Temporary Group Assignments
- ◆ Modify Temporary Group Assignments
- ◆ Reset Temporary Group Assignment State
- ◆ View Temporary Group Assignments
- ◆ Add Object to Group
- ◆ Remove Object from Group

The target group and users must belong to the same ActiveView.

NOTE

- ◆ You cannot create a temporary group assignment for a user who is already a member of the target group. If you try to create a temporary group assignment for a user who is already a member of the target group, DRA displays a warning message and does not allow you to create a temporary group assignment for the user.
 - ◆ If you create a temporary group assignment for a user who is not a member of the target group, DRA removes the user from the group when the temporary group assignment expires.
-

Example:

Bob, the HR manager, notifies John, a help-desk administrator, that the company has contracted a temporary employee named Joe for a specific period of time to complete a project. John does the following:

- ◆ Creates a temporary group assignment (TGA)
- ◆ Adds an HR group for temporary employees to the TGA
- ◆ Adds Joe as a member of the temporary employee group
- ◆ Sets the TGA duration for one month (07/03/2019 to 08/02/2019)

Expected result:

By default, when the TGA expires, Joe's membership will be removed from the HR group. The TGA will remain available for seven days unless John selected the option to **Keep this temporary group assignment for future use**.

For more information about creating and using temporary group assignments, see the [DRA User Guide](#).

19 DRA Dynamic Groups

A dynamic group is one whose membership changes based on a defined set of criteria that you configure in the group's properties. You can make any group dynamic or remove the dynamic filter from any group that has it configured. This feature also provides the capability to add group members to a static list or to an excluded list. Group members in these lists will not be impacted by the dynamic criteria.

If you revert a dynamic group back to a regular group, any members in the Static Member List are added to the group's membership and excluded members and dynamic filters are ignored. You can make existing groups dynamic or create a new dynamic group in both the Delegation and Configuration Console and in the Web Console.

To make a group dynamic:

1 Locate the group in applicable console.

- ◆ Delegation and Configuration: Go to **All My Managed Objects > Find Now**.

NOTE: To enable the Query Builder, click **Browse** and select a domain, container, or OU.

- ◆ Web Console: Go to **Management > Search**.

2 Open the group's Properties, and select **Make group dynamic** in the Dynamic Member Filter tab.

3 Add the desired LDAP and virtual attributes to filter group membership.

4 Add any desired static or excluded members to the dynamic group, and apply your changes.

To make a new dynamic group:

- ◆ **Delegation and Configuration:** Right-click the domain or sub-node in All My Managed Objects, and select **New > Dynamic Group**.

- ◆ **Web Console:** Go to **Management > Create > New Dynamic Group**.

20 How Event Stamping Works

When you configure an attribute for an object type, and DRA performs one of the supported operations, that attribute will be updated (stamped) with DRA specific information, including who performed the operation. This causes AD to generate an audit event for that attribute change.

As an example, assume you selected the attribute `extensionAttribute1` as your user attribute, and you have AD DS auditing configured. Whenever an assistant administrator updates a user, DRA will update the `extensionAttribute1` attribute with Event Stamping data. This means that along with the AD DS events for each attribute that the assistant administrator updated (e.g., description, name, etc.) there will be an additional AD DS event for the `extensionAttribute1` attribute.

Each of these events contain a Correlation ID that is the same for each changed attribute that was changed when the user was updated. This is how applications can associate the Event Stamping data with the other attributes that were updated.

For steps to enable Event Stamping, see [Enable Event Stamping in DRA](#).

For an example of an AD DS event and supported operation types, see the following:

- ♦ [“The AD DS Event” on page 183](#)
- ♦ [“Supported Operations” on page 184](#)

The AD DS Event

You will see an event such as this in the Windows Security event log any time DRA executes a supported operation.

LDAP Display Name:	<code>extensionAttribute1</code>
Syntax (OID): 2.5.5.12	2.5.5.12
Value:	<code><dra-event user="DRDOM300\drauseradmin" sid="S-1-5-21-53918190-1560392134-2889063332-1914" tid="E0E257E6B4D24744A9B0FE3F86EC7038" SubjectUserSid="S-1-5-21-4224976940-2944197837-1672139851-500" ObjectDN="CN=admin_113,OU=Vino_113,DC=DRDOM113,DC=LAB"/>+a+02ROO+bJbhyPbR4leJpKWCGTp/KXdqI7S3EBhVyniE7iXvxlT6eB6IdcXQ5StkbIAHJgKzLN5FCOM5fZclTxyAPLWhbst aA7ZA0VbVC9MGIVlaAcjl3z7mpF9GKXsfDogbSeNImHliXvH5KpOX3/29AKMPj/zvf6YuczooS=</code>

The event value consists of two pieces. The first is an XML string containing the Event Stamping data. The second is a signature of the data that can be used to validate that the data was generated by DRA. To validate the signature, an application must have the public key for the signature.

The XML string consists of the following information:

User	The assistant administrator who performed the operation
Sid	The SID of the assistant administrator who performed the operation
Tid	The DRA auditing transaction ID to ensure each event is unique
SubjectUserSid	The SID of the DRA service account or access account that updated AD
ObjectDN	The distinguished name of the object that was modified

Supported Operations

User	<ul style="list-style-type: none">◆ Create◆ Rename◆ Modify◆ Clone
Group	<ul style="list-style-type: none">◆ Create◆ Rename◆ Modify◆ Clone
Contact	<ul style="list-style-type: none">◆ Create◆ Rename◆ Modify◆ Clone
Computer	<ul style="list-style-type: none">◆ Create◆ Enable◆ Disable◆ Rename◆ Modify
Organizational Unit	<ul style="list-style-type: none">◆ Create◆ Rename◆ Clone

21 BitLocker Recovery Password

Microsoft BitLocker stores its recovery passwords in Active Directory. Using the DRA BitLocker Recovery feature, you can delegate powers to assistant administrators to find and recover lost BitLocker passwords for end users.

IMPORTANT: Before using the BitLocker Recovery Password feature, ensure that your computer is assigned to a domain and BitLocker is turned-on.

Viewing and Copying a BitLocker Recovery Password

If the BitLocker password for a computer is lost, it can be reset using the Recovery Password key from the computer's properties in Active Directory. Copy the password key and provide it to the end user.

To view and copy the recovery password:

- 1 Launch the **Delegation and Configuration** console, and expand the tree view structure.
- 2 In the **Account and Resource Management** node, navigate to **All My Managed Objects > Domain > Computers**.
- 3 In the computers list, right-click the required computer, and select **Properties**.
- 4 Click the **BitLocker Recovery Password** tab to view the BitLocker recovery password.
- 5 Right-click the BitLocker recovery password, click **Copy**, and then paste the text onto required text file or spreadsheet.

Finding a Recovery Password

If the name of a computer was changed, the Recovery Password must be searched for in the domain using the first eight characters of the Password ID.

NOTE: To search for the Recovery Password, the assistant administrator must have the **View BitLocker recovery password** power on the domain containing the delegated computer objects.

To find a recovery password by using a password ID:

- 1 Launch the **Delegation and Configuration** console, and expand the tree view structure.
- 2 In the **Account and Resource Management** node, navigate to **All My Managed Objects**, right-click on the **Managed Domain**, and then click **Find BitLocker Recovery Password**.
To find the first eight characters of the recovery password, see [Viewing and Copying a BitLocker Recovery Password](#).
- 3 In the **Find BitLocker Recovery Password** page, paste the copied characters in the search field, and then click **Search**.

22 Recycle Bin

You can enable or disable the Recycle Bin for each Microsoft Windows domain or objects within those domains, controlling the management of accounts across your enterprise. If you enable the Recycle Bin and then delete a user account, group, dynamic distribution group, dynamic group, resource mailbox, contact, or computer account, the Administration server disables the selected account and moves it to the Recycle Bin container. Once DRA moves the account to the Recycle Bin, the account does not display in the ActiveViews to which it belonged. If you delete a user account, group, contact, or computer account when the Recycle Bin is disabled, the Administration server permanently deletes the selected account. You can disable a Recycle Bin that contains previously deleted accounts. However, once the Recycle Bin is disabled, these accounts are no longer available in the Recycle Bin node.

Assigning Recycle Bin Powers

To allow an assistant administrator to permanently delete accounts from the All My Managed Objects node as well as the Recycle Bin, assign the relevant power from the following list:

- ◆ Delete User Account Permanently
- ◆ Delete Group Permanently
- ◆ Delete Computer Permanently
- ◆ Delete Contact Permanently
- ◆ Delete Dynamic Distribution Group Permanently
- ◆ Delete Dynamic Group Account Permanently
- ◆ Delete Resource Mailbox Permanently
- ◆ Delete Shared Mailbox Permanently
- ◆ Delete Azure User Account Permanently
- ◆ Delete Group Managed Service Account Permanently

If multiple Administration servers manage different subtrees in the same Microsoft Windows domain, you can use the Recycle Bin to view any deleted account from this domain regardless of which Administration server manages that account.

Using the Recycle Bin

Use the Recycle Bin to permanently delete accounts, restore accounts, or view properties of deleted accounts. You can also search for specific accounts and track how many days a deleted account has been in the Recycle Bin. A Recycle Bin tab is also included in the Properties window for a selected domain. From this tab you can disable or enable the Recycle Bin for the entire domain or for specific objects, as well as schedule a Recycle Bin cleanup.

Use the **Restore All** or **Empty Recycle Bin** options to quickly and easily restore or delete these accounts.

When you restore an account, DRA reinstates the account, including all permissions, power delegations, policy assignments, group memberships, and ActiveView memberships. If you permanently delete an account, DRA removes this account from the Active Directory.

To ensure secure account deletion, only assistant administrators who have the following powers can permanently delete the accounts from the Recycle Bin:

- ◆ Delete User Account Permanently
- ◆ Delete User from Recycle Bin
- ◆ Delete Group Account Permanently
- ◆ Delete Group from Recycle Bin
- ◆ Delete Computer Account Permanently
- ◆ Delete Computer from Recycle Bin
- ◆ Delete Contact Account Permanently
- ◆ Delete Contact from Recycle Bin
- ◆ Delete Dynamic Distribution Group Permanently
- ◆ Delete Dynamic Distribution Group from Recycle Bin
- ◆ Delete Dynamic Group Permanently
- ◆ Delete Dynamic Group from Recycle Bin
- ◆ Delete Resource Mailbox Permanently
- ◆ Delete Resource Mailbox from Recycle Bin
- ◆ Delete Shared Mailbox Permanently
- ◆ Delete Shared Mailbox from Recycle Bin
- ◆ View all Recycle Bin Objects

To restore an account from the Recycle Bin, assistant administrators must have the following powers in the OU that contains the account:

- ◆ Restore User From Recycle Bin
- ◆ Restore Group from Recycle Bin
- ◆ Restore Dynamic Distribution Group from Recycle Bin
- ◆ Restore Dynamic Group from Recycle Bin
- ◆ Restore Resource Mailbox from Recycle Bin
- ◆ Restore Shared Mailbox from Recycle Bin
- ◆ Restore Computer from Recycle Bin
- ◆ Restore Contact from Recycle Bin
- ◆ View all Recycle Bin Objects

NOTE

- ◆ If you delete an assistant administrator account to the Recycle Bin, DRA continues to display the ActiveView and role assignments for this account. Instead of displaying the name of the deleted assistant administrator account, DRA displays the security identifier (SID). You can remove these assignments before you permanently delete the assistant administrator account.

- ♦ DRA deletes the home directory after you delete the user account from the Recycle Bin.
 - ♦ If you delete a user who has an Office 365 license, the user account goes to the Recycle Bin and the license is removed. If you later restore the user account, the Office 365 license will also be restored.
-

VIII Client Customization

You can customize the Delegation and Configuration client and the Web Console. The former requires physical or remote access and account credentials. The latter requires the server URL and account credentials to log in from a Web browser.

- ♦ [Chapter 23, “Delegation and Configuration Client,” on page 193](#)
- ♦ [Chapter 24, “Web Client,” on page 205](#)

23 Delegation and Configuration Client

This section includes information to help you customize the Delegation and Configuration client, which includes understanding how to create custom property pages, how to create custom tools in DRA that can run on client and server computers in the network, and how to customize the configuration of the user interface.

Customizing Property Pages

You can customize and extend the Delegation and Configuration console by implementing custom properties. Custom properties enable you to add proprietary account and OU properties, such as Active Directory schema extensions and virtual attributes, to specific wizards and property windows. These extensions allow you to customize DRA to meet your specific requirements. Using the New Custom Page wizard in the Delegation and Configuration console, you can quickly and easily create a custom page to extend the appropriate user interface.

If your assistant administrators require unique powers to securely manage the custom page, you can also create and delegate custom powers. For example, you may want to limit user account management to properties on the custom page only. For more information, see [Implementing Custom Powers](#).

- ♦ [“How Custom Property Pages Work”](#) on page 193
- ♦ [“Supported Custom Pages”](#) on page 194
- ♦ [“Supported Custom Property Controls”](#) on page 195
- ♦ [“Working with Custom Pages”](#) on page 196
- ♦ [“Creating Custom Property Pages”](#) on page 197
- ♦ [“Modifying Custom Properties”](#) on page 198
- ♦ [“Identifying Active Directory Attributes Managed With Custom Pages”](#) on page 198
- ♦ [“Enabling, Disabling, and Deleting Custom Pages”](#) on page 198
- ♦ [“Command-Line Interface”](#) on page 199

How Custom Property Pages Work

User interface extensions are custom pages DRA displays in the appropriate wizard and properties windows. You can configure custom pages to expose Active Directory attributes, schema extensions, and virtual attributes in the Delegation and Configuration console.

When you select any supported Active Directory attribute, schema extension, or virtual attribute, you can use custom pages in the following ways:

- ♦ Limit assistant administrators to manage a well-defined and controlled set of properties. This property set can include *standard properties* and schema extensions. Standard properties are Active Directory attributes exposed by default through the Accounts and Resource Management console.

- ◆ Expose Active Directory attributes other than the standard properties managed by DRA.
- ◆ Extend the Delegation and Configuration console to include proprietary properties.

You can also configure how DRA displays and applies these properties. For example, you can define user interface controls with default property values.

DRA applies custom pages to all applicable managed objects in your enterprise. For example, if you create a custom page to add Active Directory schema extensions to the Group Properties window, DRA applies the properties on this page to each managed group in a domain supporting the specified schema extensions. Each custom page requires a unique set of properties. You cannot add an Active Directory attribute to more than one custom page.

You cannot disable individual windows or tabs in the existing user interface. An assistant administrator can select a property value using either the default user interface or a custom page. DRA applies the most recently selected value for a property.

DRA provides a full audit trail for custom properties. DRA logs the following data to the Application event log:

- ◆ Changes to custom pages

IMPORTANT: You must manually configure Windows Application Log Auditing. For more information, see [Enabling and Disabling Windows Event Log Auditing for DRA](#).

- ◆ Creation and deletion of custom pages
- ◆ Exposed schema extension, Active Directory attributes, and virtual attributes included on custom pages

You can also run change activity reports to monitor configuration changes for the custom properties.

Implement and modify custom pages from the primary Administration server. During synchronization, DRA replicates custom page configurations across the Multi-Master Set. For more information, see [Configuring the Multi-Master Set](#).

Supported Custom Pages

Each custom page you create allows you to select a set of Active Directory properties, schema extensions, or virtual attributes and expose these properties as a custom tab. You can create the following types of custom pages:

Custom User Page

Allows you to display custom tabs in the following windows:

- ◆ User Properties window
- ◆ Create User wizard
- ◆ Clone User wizard

Custom Group Page

Allows you to display custom tabs in the following windows:

- ◆ Group Properties window

- ◆ Create Group wizard
- ◆ Clone Group wizard

Custom Computer Page

Allows you to display custom tabs in the following windows:

- ◆ Computer Properties window
- ◆ Create Computer wizard

Custom Contact Page

Allows you to display custom tabs in the following windows:

- ◆ Contact Properties window
- ◆ Create Contact wizard
- ◆ Clone Contact wizard

Custom OU Page

Allows you to display custom tabs in the following windows:

- ◆ OU Properties window
- ◆ Create OU wizard
- ◆ Clone OU wizard

Custom Resource Mailbox Page

Allows you to display custom tabs in the following windows:

- ◆ Resource Mailbox Properties window
- ◆ Create Resource Mailbox wizard
- ◆ Clone Resource Mailbox wizard

Custom Dynamic Distribution Group Page

Allows you to display custom tabs in the following windows:

- ◆ Dynamic Distribution Group Properties window
- ◆ Create Dynamic Distribution Group wizard
- ◆ Clone Dynamic Distribution Group wizard

Custom Shared Mailbox Page

Allows you to display custom tabs in the following windows:

- ◆ Shared Mailbox Properties window
- ◆ Create Shared Mailbox wizard
- ◆ Clone Shared Mailbox wizard

Supported Custom Property Controls

When you add an Active Directory attribute, schema extension, or virtual attribute to a custom page, you also configure the user interface control with which an assistant administrator inputs the property value. For example, you can specify property values in the following ways:

- ◆ Define specific value ranges

- ◆ Set default property values
- ◆ Indicate whether a property is required

You can also configure the user interface control to display proprietary information or instructions. For example, if you define a specific range for an employee identification number, you can configure the text box control label to display **Specify employee identification number (001 to 100)**.

Each user interface control provides support for a single Active Directory attribute, schema extension, or virtual attribute. Configure the following user interface controls based on the property type:

Type of Active Directory attribute	Supported User Interface Controls
Boolean	Check box
Date	Calendar control
Integer	Text box (default) Selection list
String	Text box (default) Selection list Object selector
Multivalued String	Selection list

Working with Custom Pages

You can create custom pages from the User Interface Extensions node. Once a page is created, you can add or remove AD attribute properties, and disable or delete the page. For each customization you want to configure, create a custom page and assign the appropriate power or role to the assistant administrator. Consider the best practices below as you start working with custom pages:

1. To ensure DRA recognizes your Active Directory attributes, schema extension attributes, or virtual attributes, restart the Administration Service on each Administration server.
2. Identify the type of custom page you want to create and the properties you want assistant administrators to manage with this custom page. You can select any Active Directory attribute, including schema extension attributes and attributes in existing DRA wizards and property windows or any virtual attribute you create. However, each custom page requires a unique set of properties. You cannot add an Active Directory attribute to more than one custom page.

Custom pages do not replace the existing user interface. For more information, see [How Custom Property Pages Work](#) and [Supported Custom Pages](#).

3. Determine how you want assistant administrators to specify these properties. For example, you may want to limit a specified property to three values. You can define an appropriate user interface control for each property. For more information, see [Supported Custom Property Controls](#).
4. Determine whether your assistant administrators need proprietary information or instructions to successfully manage these properties. For example, determine whether Active Directory requires a syntax for the property value, such as a distinguished name (DN) or an LDAP path.

5. Identify the order in which these properties should display on the custom page. You can change the display order at any time.
6. Determine how DRA should use this custom page. For example, you can add a user custom page to the New User wizard and the User Properties window.
7. Use the Assignments tab on the Assistant Admin details pane to verify that your assistant administrators have the appropriate powers for the correct set of objects. If you created custom powers for this custom page, delegate those powers to the appropriate assistant administrators.
8. Determine whether your assistant administrators need a custom power to manage the properties on this page. For example, if you add a custom page to the User Properties window, delegating the *Modify All User Properties* power may give an assistant administrator too much power. Create any custom powers needed to implement your custom page. For more information, see [Implementing Custom Powers](#).
9. Using your answers from steps above, create the appropriate custom pages.
10. Distribute information about the custom property pages you implemented to the appropriate assistant administrators, such as your Help Desk.

To implement property customization, you must have the powers included in the DRA Administration role. For more information about custom pages, see [How Custom Property Pages Work](#).

Creating Custom Property Pages

You can create different custom properties by creating different custom pages. By default, new custom pages are enabled.

When you create a custom page, you can disable it. Disabling a custom page hides it from the user interface. If you are creating multiple custom pages, you may want to disable the pages until your customizations are tested and complete.

NOTE: Computer accounts inherit Active Directory attributes from user accounts. If you extend your Active Directory schema to include additional attributes for user accounts, you can select these attributes when you create a custom page to manage computer accounts.

To create a custom property page:

1. Navigate to **Configuration Management > User Interface Extensions** node.
2. On the Task menu, click **New**, and then click the appropriate menu item for the custom page you want to create.
3. On the General tab, type the name of this custom page, and then click **OK**. If you want to disable this page, clear the **Enabled** check box.
4. For each property you want to include on this custom page, complete the following steps:
 - 4a. On the Properties tab, click **Add**.
 - 4b. To select a property, click **Browse**.
 - 4c. In the **Control label** field, type the property name DRA should use as the label for the user interface control. Ensure the control label is user-friendly and highly descriptive. You can also include instructions, valid value ranges, and syntax examples.

- 4d** Select the appropriate user interface control from the **Control type** menu.
- 4e** Select where in the Delegation and Configuration console you want DRA to display this custom page.
- 4f** To specify additional attributes, such as minimum length or default values, click **Advanced**.
- 4g** Click **OK**.
- 5** To change the order in which DRA displays these properties on the custom page, select the appropriate property, and then click **Move Up** or **Move Down**.
- 6** Click **OK**.

Modifying Custom Properties

You can change a custom page by modifying the custom properties.

To modify custom properties:

- 1** Navigate to **Configuration Management > User Interface Extensions** node.
- 2** In the list pane, select the desired custom page.
- 3** On the Tasks menu, click **Properties**.
- 4** Modify the appropriate properties and settings for this custom page.
- 5** Click **OK**.

Identifying Active Directory Attributes Managed With Custom Pages

You can quickly identify which Active Directory properties, schema extensions, or virtual attributes are managed using a particular custom page.

To identify Active Directory properties managed using custom pages:

- 1** Navigate to **Configuration Management > User Interface Extensions** node.
- 2** In the list pane, select the desired custom page.
- 3** In the details pane, click the **Properties** tab. To view the details pane, click **Details** on the View menu.
- 4** To verify how DRA displays and applies a property, select the appropriate Active Directory attribute, schema extension, or virtual attribute from the list, and then click the **Properties** icon.

Enabling, Disabling, and Deleting Custom Pages

When you enable a custom page, DRA adds this custom page to the associated wizards and windows. To specify which wizards and windows display a custom page, modify the custom page properties.

NOTE: To ensure each custom page exposes a unique set of properties, DRA does not enable custom pages that contain properties exposed on other custom pages.

When you disable a custom page, DRA removes the custom page from the associated wizards and windows. DRA does not delete the custom page. To ensure a custom page never displays in the user interface, delete the custom page.

When you delete a custom page, DRA removes the custom page from the associated wizards and windows. You cannot restore a deleted custom page. To temporarily remove a custom page from the user interface, disable the custom page.

To enable, disable, or delete a custom page, navigate to **Configuration Management > User Interface Extensions** node, and select the desired action in the Tasks or right-click menu.

Command-Line Interface

The CLI enables you to access and apply powerful Administration product capabilities using commands or batch files. With the CLI, you can issue one command to implement changes across multiple objects.

For example, if you need to relocate the home directories of 200 employees to a new server, using the CLI, you could enter the following single command to change all 200 user accounts:

```
EA USER @GroupUsers(HOU_SALES),@GroupUsers(HOU_MIS) UPDATE  
HOMEDIR: \\HOU2\USERS\@Target ( )
```

This command directs DRA to change the home directory field of each of the 200 user accounts in the HOU_SALES and HOU_MIS groups to \\HOU2\USERS\user_id. To accomplish this task with the native Microsoft Windows administration tools, you would need to perform a minimum of 200 separate actions.

NOTE: The CLI tool will be deprecated in future releases as more features are added to PowerShell.

Custom Tools

Custom tools can be used to invoke any application to be run on client and server computers in the network by selecting any Active Directory account that is managed in DRA.

DRA supports two types of custom tools:

- ◆ Custom tools that launch common desktop utilities, such as Microsoft Office
- ◆ Custom tools that you create and distribute to each DRA client computer

You can create a custom tool that launches an anti-virus scan from all computers where DRA client is installed. You can also create a custom tool that launches an external application or a tool that requires DRA to update a script periodically. These periodic updates can be changes in the configuration or changes in the business rule. Subsequently, after the periodic updates, DRA replicates custom tools from the primary Administration server to any secondary Administration servers and DRA client computers.

To understand how custom tools get replicated in the server multi-master set, see [File Replication](#).

Creating Custom Tools

You can create custom tools in the DRA Primary server by associating to either a selected Active Directory object or all Active Directory objects displaying in that create custom tool wizard. The same will be replicated to secondary servers in the MMS and to the DRA clients through file replication.

A new custom tool will create a menu and submenu, if required, to invoke the operation against the associated Active Directory object(s) in DRA.

You can delegate powers to assistant administrators to create and execute custom tools, and to access and run the application.

When creating a custom tool, you need to input the parameters, as follows:

General tab

1. **Name:** Any required customer name for the tool.
2. **Menu and Submenu:** To create a menu item for a new custom tool, enter the menu title in the **Menu and Submenu Structure** field. When you create a custom tool and select the object, DRA displays the custom tool menu item using the menu and submenu structure that you specify in the Tasks menu, the Shortcut menu, and the DRA toolbar.

Sample Menu and SubMenu structure: Type the menu item name, a backslash (\) character, and then the submenu item name.

To have short cut key: Type an ampersand (&) character before the name of the menu item.

- a. Example: `SendEmail\ApproveAction` --- `SendEmail` is the menu and `ApproveAction` is submenu with the with first letter "A" in `ApproveAction` being the short cut key enabled.
3. **Enabled:** Check this box to activate the custom tool.
 4. **Description:** You can add any required description value.
 5. **Comment:** You can add any required comments to the custom tool.

Supported Objects tab

Select the required AD object or all the AD objects to which the created custom tool should get associated.

Current supported custom tool options include: Managed Domain, Containers, Users, Contacts, Groups, Computers, Organizational Unit, and Published Printers.

NOTE: Other newly introduced objects like Resource Mailbox, Dynamic Group, and Exchange Dynamic Group are not supported with Custom Tools.

Application Settings tab

Location of the application: You need to provide the path/location of the application where it is installed, either by copying and pasting the exact application path or through the **Insert** option.

This same path must already exist on all DRA servers in the MMS. If required, you can use [File Replication](#) to upload and replicate a file to a usable path on MMS servers before creating a new custom tool.

You can also use DRA variables, environment variables, and registry values to specify the location of the external application in the Location of the application field. To use these variables, click **Insert**, and select the variable you wish to use.

After you insert the variable, type a backslash (\) character, and then specify the rest of the path of the application, including the application executable file name.

Examples:

- ◆ *Example 1:* To specify the location of an external application that the custom tool will run, select the environmental variable `{%PROGRAMFILES%}` and then specify the rest of the path of the application in the Location of the application field: `{%PROGRAMFILES%}\ABC Associates\VirusScan\Scan32.exe`

NOTE: DRA provides the Office Install Directory registry value as a sample. To specify a registry key that contains a path as a value, use the following syntax:

```
{HKEY_LOCAL_MACHINE\SOFTWARE\MyProduct\SomeKey\ (Default)}
```

- ◆ *Example 2:* To specify the location of a custom script file that the custom tool will run, select the DRA variable `{DRA_Replicated_Files_Path}`, and then specify the rest of the path of the script file in the Location of the application field:
`{DRA_Replicated_Files_Path}\cscript.vbs ; where
{DRA_Replicated_Files_Path} is the replicated file path or the
{DRAInstallDir}\FileTransfer\Replicate` the folder in the Administration server.

NOTE: Before creating the custom tool, upload the script file to the primary Administration server using the file replication feature. The file replication feature uploads the script file to the `{DRAInstallDir}\FileTransfer\Replicate` folder in the primary Administration server.

- ◆ *Example 3:* To specify the location of a DRA utility that the custom tool will run, select the DRA variable `{DRA_Application_Path}` and then specify the rest of the path of the utility in the Location of the application field: `{DRA_Application_Path}\DRADiagnosticUtil.exe ; where {DRA_Application_Path} is the location where DRA is installed.`
- ◆ *Example 4:* Simply copy and paste the location of the application along with the application file name with extension.

Parameters to pass to the application: To define a parameter to pass to an external application, copy and paste or type one or more parameters in the Parameters to pass to the application field. DRA provides parameters that you can use in the Parameters to pass to the application field. To use these parameters, click **Insert** and select the parameter or parameters you wish to use. When providing object property as a parameter, ensure that the assistant administrator has the required Read permission on the object property along with the *Execute Custom Tools* power to run the custom tool.

Examples:

- ◆ *Example 1:* To pass group name and domain name as parameters to an external application or script, select the Object Property Name and Domain Property Name parameters and specify the parameter names in the Parameters to pass to the application field: "{Object.Name}" "{Domain.\$McsName}"
- ◆ *Example 2:* To pass the input parameter "ipconfig" for the application "C:\Windows\SysWOW64\cmd.exe" just type "{C:\Windows\SysWOW64\cmd.exe}" "{ipconfig}" in that field.

Directory where the application will run: This is the location where the application needs to run in the client or server machine. You need to pass the path where the application should be executed. You can also use the "Insert" option in the same way we pass the parameter for the field "Location of the application". Other parameters in this tab are implicitly for explaining its usage.

Customizing the User Interface

There are several options to customize how the Delegation and Configuration Console is configured. Most of these options provide the capability to hide, show, or reconfigure features in the different feature panes in the application. You can also hide or show the toolbar, customize the application title, and add, remove, or reorder columns. The customization options are located in the **View** menu.

Modifying the Console Title

You can modify the information displayed in the title bar of the Delegation and Configuration console. For convenience and clarity, you can add the user name with which the console was launched and the Administration server to which the console is connected. In complex environments in which you need to connect to multiple Administration servers using different credentials, this feature helps you quickly discern which console you need to use.

To modify the console title bar:

- 1 Start the Delegation and Configuration console.
- 2 Click **View > Options**.
- 3 Select the Window Title tab.
- 4 Specify the appropriate options, and then click **OK**. For more information, click the ? icon.

Customizing List Columns

You can select which object properties DRA displays in list columns. This flexible feature allows you to customize the user interface, such as lists for search results, to better meet the specific demands of administrating your enterprise. For example, you can set columns to display the user logon name or group type, letting you quickly and effectively find and sort the data you need.

To customize list columns:

- 1 Select the appropriate node. For example, to choose which columns display when viewing search results on managed objects, select **All My Managed Objects**.
- 2 On the View menu, click **Choose Columns**.

- 3 From the list of properties available for this node, select the object properties you want to show.
- 4 To change the column order, select a column, and then click **Move Up** or **Move Down**.
- 5 To specify the column width, select a column, and then type the appropriate number of pixels in the provided field.
- 6 Click **OK**.

24 Web Client

In the Web Client, you can customize object properties, Workflow Automation forms, and the user interface branding. When implemented correctly, property and workflow customizations will help to automate assistant administrator tasks during object management and automated workflow submissions.

Customizing Property Pages

You can customize the object property forms that your assistant administrators use in their Active Directory management roles by object type. This includes creating and customizing new object pages that are based on object types that are built into DRA. You can also modify properties for the built-in object types.




Property objects are clearly defined in the Customization > Property Pages list in the Web Console, so you can easily identify which object pages are built-in, which built-in pages are customized, and which pages are not built-in and were created by an administrator.




Customizing an Object Property Page

You can customize object property forms by adding or removing pages, modifying existing pages and fields, and by creating custom handlers for property attributes. The custom handlers on a field are executed whenever that field's value is modified. The timing can be configured as well, so the administrator can specify if the handlers should be run immediately (on every key press), when the field loses focus, or after a specified time delay.

The object list in Property Pages provides operation types for each object type, Create Object and Edit Properties. These are the principal operations your assistant administrators perform in the Web Console. They perform these operations by navigating to **Management > Search** or **Advanced Search**. Here they can create objects from the Create pull-down menu or edit existing objects selected in the search results table through the Properties icon.

To customize an object property page in the Web Console:

- 1 Log in to the Web Console as DRA Administrator.
- 2 Navigate to **Administration > Customization > Property Pages**.
- 3 Select an object and operation type (Create Object or Edit Object) in the Property Pages list.
- 4 Click the **Properties** icon .
- 5 Customize the object property form by doing one or more of the following, and then applying your changes:
 - ◆ Add a new property page: **+ Add Page**
 - ◆ Reorder and delete property pages
 - ◆ Select a property page and customize the page:
 - ◆ Reorder configuration fields in the page:  

- ◆ Edit fields or subfields: 
- ◆ Add one or more fields:  or [Insert a new Field](#)
- ◆ Remove one or more fields: 
- ◆ Create custom handlers for properties by using scripts, message boxes, or queries (LDAP, DRA, or REST)

For more information about using custom handlers, see [Adding Custom Handlers](#).

Defining Custom Filters

You can use filters to customize the information that is displayed for each object type by adding the **Managed Object Browser** field to a property page. When configuring the field settings, you can add filters in the settings via the Managed Object Browser Options tab. By defining custom filters, you can restrict the information that is displayed in object browsers for assistant administrators. Assistant administrators can view only those objects that meet the filter conditions that you have defined.


To define a filter, in the Managed Object Browser Options tab, enable the **Specify Object Filters** check box. For each filter condition, specify the object type, attribute to be filtered, filter condition, and attribute value that will be used to filter the information. When you create multiple filters for the same object type, they are combined with the AND operator. With all the predefined filters in the Managed Object Browser, assistant administrators can perform the search operation.

NOTE

- ◆ Only cached attributes can be used to define filters.
 - ◆ If you create a custom handler using a custom script for the custom filter, you must also define the custom filter manually in **Managed Object Browser Options** tab for the custom handler to work.
-

Creating a New Object Property Page

To create a new object property page:

- 1 Login to the Web Console as DRA Administrator.
- 2 Navigate to **Administration > Customization > Property Pages**.
- 3 Click  **Create**.
- 4 Create the initial object properties form by defining action name, icon, object type, and operation configuration.
Create actions are added to the Create drop-down menu while Property actions display in object form when the user selects and edits an object from the search list.
- 5 Customize the new form as required. See [Customizing an Object Property Page](#).

Customizing Request Forms

Request forms, when created or modified, are saved to the Web Server. The DRA administrator manages them from **Administration > Customization > Requests**. Assistant administrators manage them from **Tasks > Requests**. These forms are used to submit automated workflows that are created in the Workflow Automation server. Form creators use these requests to further automate and improve object management tasks.

You can add and modify existing form properties and custom handlers. The interface behavior for adding and customizing properties is the same in a Workflow Automation form as it is when customizing object properties with the exception of workflow configuration options and controls for who can use the form. Reference the topics below for more information about adding and modifying properties, adding custom handlers, and understanding Workflow Automation.

- ◆ [Customizing Property Pages \(Web Client\)](#)
- ◆ [Adding Custom Handlers](#)
- ◆ [Automated Workflow](#)

Adding Custom Handlers

Custom handlers are used in DRA for property attributes to interact with each other to accomplish a workflow task and for Load and Submit customizations in a workflow, property, or create form.

Property custom handlers

A few examples of property custom handlers, include:

- ◆ querying the value of other fields
- ◆ updating field values
- ◆ toggling a field's read-only state
- ◆ showing or hiding fields based on configured variables

Page load handlers

Page load handlers typically perform initialization and are mostly used in custom property pages. They are only executed the first time a page is selected and in the case of property pages, they are executed after data is loaded from the server.

Form load handlers

Form load handlers typically perform initialization controls. They are executed only once when the form initially loads. In the case of property pages, they are executed before the server is queried for the properties of the selected object.

Form submit handlers

Form submit handlers enable users to do some type of validation and potentially cancel form submission if something is not right.

NOTE: As a best practice, avoid configuring change handlers on page and form handlers that modify the values of fields that are on different pages (tabs) than where you create the handler. In this scenario, data on a different page than the handler will not load until the assistant administrator accesses that page, which can conflict with the value being set by the change handler.

For detailed examples of using custom handlers and customizations in the Web Console, reference the “Web Console Customization” and “Workflow Customization” sections in the *Product Customization* reference on the [DRA Documentation page](#).



See the following topics for more information about custom handler behavior and how to create them:

- ◆ “Basic Steps for Creating a Custom Handler” on page 208
- ◆ “Enabling Custom JavaScript” on page 210
- ◆ “Using the Script Editor” on page 210
- ◆ “About Custom Handler Execution” on page 212




Basic Steps for Creating a Custom Handler

Before attempting to create a custom handler, ensure that custom JavaScript is enabled in the console configuration. For more information, see [Enabling Custom JavaScript](#).

The steps below begin from a pre-selected custom handler page. To get to that point, you navigate to different handlers as follows:

- ◆ Object properties custom handlers: Click the edit icon  on a property field.
- ◆ Page load handlers: Select the page’s Properties. For example, **General** >  **More Options** > **Properties**.
- ◆ Form Load or Form Submit handlers: Click the **Form Properties** button on a selected Workflow form, a Create Object page, or an Edit Properties page.

Creating a custom handler:

- 1 Select the applicable handler tab based on the property or page you are customizing:
 - ◆ Custom Handlers
 - ◆ Page Load Handlers
 - ◆ Form Load Handlers
 - ◆ Form Submit Handlers
- 2 Enable the handler page    and do one of the following:
 - ◆ **Property field custom handler:**
 1. Select an execution time. Normally, you would use the second option.

The execution time controls when the change handlers are executed in response to user input. Note that this setting does not apply when the field’s value is updated by another custom handler using the `draApi.fieldValues` interface.
 2. Click **+ Add** and choose a custom handler from the **Add Custom Handler** menu.
 - ◆ **Page or form handler:** Click **+ Add** and choose a custom handler from the **Add Custom Handler** menu.

NOTE: Typically, you may only require one custom handler, but you can use more than one handler. Multiple handlers are executed sequentially in the order listed. If you want to change the order of handlers or skip a handler that is not needed, you can add flow control APIs in the script.

- 3 You will need to configure each custom handler that you add to the page. Configuration options vary by handler type. The script editor has built-in Help and dynamic Intellisense code-completion assistance that also references snippets from the Help. For more information about using these features, see [Using the Script Editor](#).

You can create your own handler types.

- ◆ **LDAP or REST Query handlers:**

1. If you want your query to be based on static values, define **Connection Information** and **Query Parameters**.

NOTE: For LDAP queries, you can require a specific authentication type in Connection Information settings:

- ◆ **Default Account:** Authenticates with a DRA Server login.
- ◆ **Managed Domain Override Account:** Authenticates to Active Directory through the existing Managed Domain Override Account.
- ◆ **LDAP Override Account:** Authenticates through an LDAP Override Account, as opposed to a domain account from a managed domain. To use this option, the account must first be enabled in the Delegation and Configuration Console. For more information, see [Enable LDAP Override Authentication](#).

If you want your query to be dynamic, enter placeholder values in the mandatory fields. This is required for the handler to execute. The script will override the placeholder values.

NOTE: You can also configure Headers and Cookies for the REST Query.

2. In Pre-Query Action, use the script editor to write custom JavaScript code that will execute before the query is submitted. This script has access to all the connection information and query parameters and can modify any of them to customize the query. For example, setting query parameters based on values the user has entered in the form.
 3. In the Post-Query Action, include script to process the results of the query. Common tasks include checking for errors, updating form values based on the results returned, and validating object uniqueness based on the number of objects returned by the query.
- ◆ **Script:** Insert custom JavaScript code to build the script.
 - ◆ **DRA Query:** Specify the JSON payload in the Query Parameters tab. The payload format must match the VarSet key or value pairs that will be sent to the DRA server. Similar to REST and LDAP queries, you can specify a Pre-Query Action that can be used to modify the payload before it is submitted to the server and a Post-Query Action to process the results.

- ◆ **Message Box handlers:** After defining the properties of the message box itself, you can also write the JavaScript segments for **Before-Show Action** and **After-Close Action**.

These actions are optional. Before-Show is used to customize any of the message box properties before it is shown to the user and the After-Close Action is used to process the user's button selection and perform any additional logic based on it.

- 4 Click **OK** to save the handler.

For detailed examples of using custom handlers and customizations in the Web Console, reference the “Web Console Customization” and “Workflow Customization” sections in the *Product Customization* reference on the [DRA Documentation page](#)

Enabling Custom JavaScript

For security reasons, custom JavaScript is disabled by default. Enabling custom JavaScript allows administrators to write snippets of JavaScript code, which the Web Console will execute as-is. You should only enable this exception if you understand and accept the risks.

To enable customizations to include custom JavaScript code:

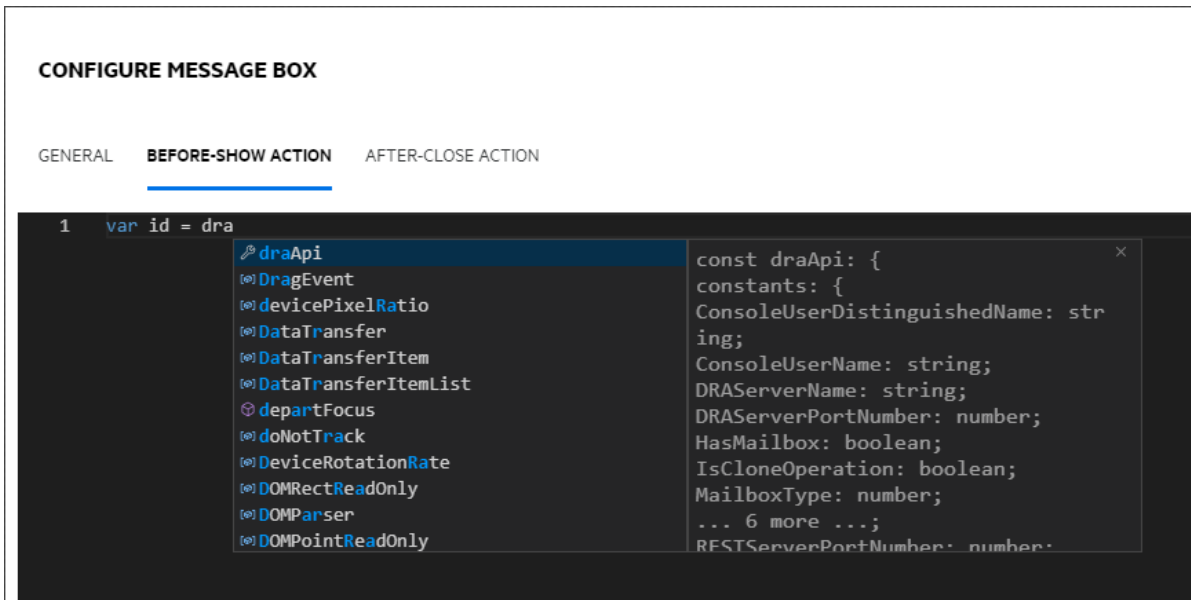
- 1 Navigate to the `C:\ProgramData\NetIQ\DRARESTProxy` location.
- 2 Open the `restProxy.config` file.
- 3 Add `allowCustomJavaScript="true"` to the `<consoleConfiguration>` element.

Using the Script Editor

The script editor enables free-form typing and pasting of JavaScript methods using DRA APIs to create custom handlers in DRA. The editor includes dynamic Intellisense code-completion and a fly-out Help panel to assist you when writing the script.

Intellisense Code-Completion

Intellisense in the script editor provides selectable code-completion snippets, tab-completion, and fly-out panels of API summaries with descriptions of the APIs.



NOTE: Intellisense code-completion is dynamic. This means that it can provide you with syntax options based on the type of handler you are defining the script for, but it also stores strings previously entered by the user and provides those prompts as well.

Script Editor Help

When you click the **?** **HELP** option in the script editor, a panel opens that explains the general purpose of custom handler APIs, where they are used, and lists the APIs with descriptions of their functions by API type:

- ◆ Global APIs include:
 - ◆ Form Access
 - ◆ Flow Control
 - ◆ Constants
- ◆ Message Box APIs include:
 - ◆ Before-Show Action
 - ◆ After-Close Action
- ◆ Query APIs include:
 - ◆ Query Results
 - ◆ DRA Query
 - ◆ LDAP Query
 - ◆ REST Query

About Custom Handler Execution

DRA provides the ability to customize web form behavior at several points in the form's execution life-cycle through custom handlers. Each type of custom handler has a specific execution window which in turn affects the scope of object data available during the execution of the customization, as follows:

1. *Form load handlers.* Executed when the form loads prior to the collection of object attributes that the form is connected to. These handlers do not have access to attribute values for the target object.
2. *Page load handlers.* DRA executes page load handlers the first time a page of a form is accessed. These handlers are guaranteed access to attribute values for the target object that are contained on that page.
3. *Attribute handlers.* DRA executes attribute handlers when an attribute value on the form is accessed. Furthermore, each form attribute can be configured to execute its custom handlers at one of three specific points during the user's interaction: (1) immediately (when the attribute gains focus), (2) when the attribute loses focus, or (3) a specified amount of time after the attribute loses focus.
4. *Form submit handlers.* Form Submit handlers are executed when the form is saved or changes are applied to the form.

Customizing User Interface Branding

You can customize the title bar of the DRA Web Console with your own title and logo image. The placement is directly to the right of the DRA product name. Since this location is also used for top-level navigation, it is hidden by the top-level DRA navigation links after logging in. However, the browser tab continues to display the customized title.

To customize the branding of the DRA Web Console:

- 1 Log in to the Web Console as DRA Administrator.
- 2 Navigate to **Administration > Configuration > Branding**.
- 3 If you are adding a company logo image, save the logo image on the Web Server in `inetpub\wwwroot\DRAClient\assets`.
- 4 Update the configuration, as applicable, for the Masthead and Login tiles.
If you want to add a notice for assistant administrators at login, turn on the **Show a notification modal at login** button. Update the configuration for this notification and click **PREVIEW** to see what this notification will look like at login.
- 5 When all changes are complete, click **Save**.

IX Tools and Utilities

These sections have information about the ActiveView Analyzer Utility, Diagnostic Utility, Deleted Object Utility, the Health Check Utility, and the Recycle Bin Utility provided with DRA.

- ♦ [Chapter 25, “ActiveView Analyzer Utility,” on page 215](#)
- ♦ [Chapter 26, “Diagnostic Utility,” on page 219](#)
- ♦ [Chapter 27, “Deleted Objects Utility,” on page 221](#)
- ♦ [Chapter 28, “Health Check Utility,” on page 225](#)
- ♦ [Chapter 29, “Recycle Bin Utility,” on page 227](#)

25 ActiveView Analyzer Utility

Each DRA ActiveView contains one or more rules, which apply to Active Directory (AD) objects managed by a DRA multi-master set. The ActiveView Analyzer Utility is used to monitor the processing time for each DRA ActiveView rule as it is applied to AD objects within a specific DRA operation. During a DRA operation, the DRA server compares the target objects of that operation against every rule in every ActiveView. DRA then creates a results list containing all matching rules. The ActiveView Analyzer calculates how much time was spent processing each rule as it is applied to a DRA operation.

With this information, you can diagnose ActiveView issues by checking for anomalies with ActiveView processing time, including time spent processing on unused ActiveViews. The utility also simplifies finding duplicate ActiveViews.

After running a data collection and viewing a report, you may find it necessary to modify the rules of one or more ActiveViews.

You can access the ActiveView Analyzer Utility from any DRA Administration server. However, you should run the ActiveView Utility on the Administration server where you are experiencing the issue.

To access the ActiveView Analyzer Utility, log onto the Administration server with DRA Administration role privileges and navigate to **NetIQ Administration > ActiveView Analyzer Utility** from the Start menu. You can also launch `ActiveViewAnalyzer.exe` from the DRA installed path `Program Files (x86)\NetIQ\DRA\X64`.

Use this utility to perform the following:

- ◆ Collect data on ActiveViews
- ◆ Generate an analyzer report

Example

Paul, who is an assistant administrator, notifies Bob, a DRA administrator, that creating users seems to be taking longer than usual. Bob decides to start the ActiveView analyzer on Paul's user object and then has Paul create a user. After the collection, Bob generates an analysis report and notices that a rule named Share MBX takes 50ms to enumerate. Bob identifies the ActiveView that contains the rule and after changing the rule, observes that the problem is resolved.

Starting an ActiveView Data Collection

With the ActiveView Analyzer Utility, you can collect data on ActiveViews from actions performed on them by assistant administrators. This data can then be viewed in an Analyzer report. To collect the data, you need to specify the assistant administrator to collect data on and then start an ActiveView collection.

NOTE: The assistant administrator that you want to collect data on must be connected to the same DRA server that the Analyzer is running on.

To start an ActiveView collection:

- 1 Click **Start > NetIQ Administration > ActiveView Analyzer Utility**.
- 2 In the ActiveView Analyzer page, specify the following:
 - 2a **Target DRA Server:** The DRA server that collects performance data on the Assistant Admin operations.
 - 2b **Target Assistant Administrator:** Click browse and select an assistant administrator who you want to collect data on.
 - 2c **Monitoring Duration:** Specify the total number of hours required to collect analyzer data. After it exceeds the specified time, data collection will be stopped.
- 3 Click **Start Collection** to collect ActiveView data.

After starting the ActiveView data collection, the utility clears the existing data and displays the latest status.
- 4 (Optional) You can stop the data collection manually before the scheduled duration has ended and still generate a report. Click **Stop Collection** to cease recording Assistant Admin operations on ActiveViews.
- 5 (Optional) To get the latest status, click **Collection Status**.

IMPORTANT: If you stop the collection and change the assistant administrator or restart a data collection for the same assistant administrator, the ActiveView Analyzer clears the existing data. You can only have Analyzer data for one assistant administrator in the database at a time.

Generating an Analyzer Report

Before generating an analyzer report, ensure that you stop collecting data.

In the ActiveView Analyzer page, the list of operations performed by the assistant administrator are displayed. To generate an analyzer report:

- 1 Click **Select Report** and then choose the report that you want to view.
- 2 Click **Generate Report** to generate an analysis report with ActiveView operation details such as affected AD objects by the operation, ActiveView managing the listed objects, matched, unmatched, and duration to process each individual ActiveView rule.

Using the report, you can analyze which rules are taking more time to perform operations, and then decide if any of them should be modified in or deleted from their respective ActiveViews.
- 3 (Optional) Mouse over the grid, right-click, and then use the copy menu to copy the report to a clipboard. From the clipboard, the column headers and data can be pasted to another application such as Notepad or Excel.

Identifying the Performance of Objects

To identify the performance of all objects managed by an ActiveView or rule:

- 1 Launch the Delegation and Configuration Console.
- 2 Navigate to **Delegation Management**, and click **Manage ActiveViews**.
- 3 Run a search to locate a specific ActiveView.

From here, you can find the rule or object that has an issue and make modifications.

- ♦ Double-click the ActiveView and select **Rules** to list the rules. You can modify a specific rule from the right-click menu.
 - ♦ Right-click the ActiveView and select **Show Managed Objects** to list the objects. You can modify an object from the right-click > **Properties**.
- 4 Make changes to the rule or managed object and verify if those changes solve the problem.

26 Diagnostic Utility

The Diagnostic Utility gathers information from your Administration server to help diagnose issues with DRA. Use this utility to provide log files to your Technical Support representative. The Diagnostic Utility provides a wizard interface that guides you through setting log levels and collecting diagnostic information.

You can access the Diagnostic Utility from any Administration server computer. However, you should run the Diagnostic Utility on the Administration server where you are experiencing the issue.

To access the Diagnostic Utility, log on to the Administration server computer using an administrator account that has local administrator rights and open the utility from Administration program group in the Windows Start menu.

For more information about using this utility, contact [Technical Support](#).

27 Deleted Objects Utility

This utility allows you to enable incremental accounts cache refresh support for a specific domain when the domain access account is not an administrator. If the domain access account does not have read permissions on the Deleted Objects container in the domain, DRA cannot perform an incremental accounts cache refresh.

You can use this utility to perform the following tasks:

- ◆ Verify that the specified user account or group has read permissions on the Deleted Objects container in the specified domain
- ◆ Delegate or remove read permissions to a specified user account or group
- ◆ Delegate or remove the Synchronize directory service data user right to a user account
- ◆ Display security settings for the Deleted Objects container

You can run the Deleted Objects Utility file (`DraDelObjsUtil.exe`) from the Program Files (`(x86)\NetIQ\DRA`) folder on your Administration server.

Required Permissions for Deleted Objects Utility

To use this utility, you must have the following permissions:

If you want to ...	You need this permission ...
Verify account permissions	Read Permissions access to the Deleted Objects container
Delegate read permissions on the Deleted Objects container	Administrator permissions in the domain where the Deleted Objects container is located
Delegate the Synchronize directory service data user right	Administrator permissions in the domain where the Deleted Objects container is located
Remove previously delegated permissions	Administrator permissions in the domain where the Deleted Objects container is located
Display security settings for the Deleted Objects container	Read Permissions access to the Deleted Objects container

Syntax for Deleted Objects Utility

```
DRADELOBJSUTIL /DOMAIN:DOMAINNAME [/DC:COMPUTERNAME] {/  
DELEGATE:ACCOUNTNAME | /VERIFY:ACCOUNTNAME | /REMOVE:ACCOUNTNAME | /  
DISPLAY [/RIGHT]}
```

Options for Deleted Objects Utility

You can specify the following options:

<i>/DOMAIN: domain</i>	Specifies the NETBIOS or DNS name of the domain where the Deleted Objects container is located.
<i>/SERVER: computername</i>	Specifies the name or IP address of the domain controller for the specified domain.
<i>/DELEGATE: accountname</i>	Delegates permissions to the specified user account or group.
<i>/REMOVE: accountname</i>	Removes permissions previously delegated to the specified user account or group.
<i>/VERIFY: accountname</i>	Verifies permissions of the specified user account or group.
<i>/DISPLAY</i>	Displays security settings for the Deleted Objects container in the specified domain.
<i>/RIGHT</i>	Ensures the specified user account or group has the Synchronize directory service data user right. You can use this option to delegate or verify this right. The Synchronize directory service data user right allows the account to read all objects and properties in the Active Directory.

NOTE

- ◆ If the name of the user account or group you want to specify contains a space, enclose the account name in quotation marks. For example, if you want to specify the Houston IT group, type "Houston IT".
 - ◆ When specifying a group, use the pre-Windows 2000 name for that group.
-

Examples for Deleted Objects Utility

The following examples demonstrate sample commands for common scenarios.

Example 1

To verify that the MYCOMPANY\JSmi th user account has read permissions on the Deleted Objects container in the hou.mycompany.com domain, enter:

```
DRADELOBSUTIL /DOMAIN:HOU.MYCOMPANY.COM /VERIFY:MYCOMPANY\JSMITH
```

Example 2

To delegate read permissions on the Deleted Objects container in the MYCOMPANY domain to the MYCOMPANY\Dr aAdmins group, enter:

```
DRADELOBSUTIL /DOMAIN:MYCOMPANY /DELEGATE:MYCOMPANY\DRAADMINS
```

Example 3

To delegate read permissions on the Deleted Objects container and the Synchronize directory service data user right in the MYCOMPANY domain to the MYCOMPANY\JSmith user account, enter:

```
DRADELOBJSUTIL /DOMAIN:MYCOMPANY /DELEGATE:MYCOMPANY\JSMITH /RIGHT
```

Example 4

To display security settings for the Deleted Objects container in the hou.mycompany.com domain using the HQDC domain controller, enter:

```
DRADELOBJSUTIL /DOMAIN:HOU.MYCOMPANY.COM /DC:HQDC /DISPLAY
```

Example 5

To remove read permissions on the Deleted Objects container in the MYCOMPANY domain from the MYCOMPANY\DraAdmins group, enter:

```
DRADELOBJSUTIL /DOMAIN:MYCOMPANY /REMOVE:MYCOMPANY\DRAADMINS
```


28 Health Check Utility

The DRA Health Check Utility is a standalone application that is packaged with the DRA installation kit. You use the Health Check Utility post install, and pre and post-upgrade, to verify, validate, and inform the status of components and processes for the DRA Server, the DRA Web Site, and DRA Clients. You can also use it to install or update a product license, back up the AD LDS Instance prior to a product upgrade, view descriptions of the checks, and fix issues or identify actions that need to be taken to fix issues and then re-validate them.

The Health Check Utility is accessible in the DRA program folder after executing the `NetIQAdminInstallationKit.msi` installer.

You can run the Health Check Utility at any time by executing the `NetIQ.DRA.HealthCheckUI.exe` file. When the application opens, you can choose to do a specific operation, run checks on specific components, or run checks on all components. See below for useful functions you do using the Health Check Utility:

Function	User Actions
Select All or Unselect All	Use the toolbar or File menu options to Select or Unselect all check items, or select individual check boxes to run specific checks.
Run Selected Checks	Use this toolbar or File menu option to run the selected checks (all or specific).
Save or Write Results	Use this toolbar or File menu option to create and save a detailed report for the checks that are run.
Run This Check	Select an item title to see a description of the check, and then click this toolbar icon to run the check. For example, to run one of the following operations: <ul style="list-style-type: none">◆ License Validation (Install or update a product license)◆ AD LDS Instance Backup (Back up the AD LDS Instance)◆ Replication (Validate the Replication database)
Fix This Issue	Select an item title, and then use this toolbar option when a check has failed. If running the check again does not fix the issue, the description should include information or actions you can take to resolve the issue.

29 Recycle Bin Utility

This utility allows you to enable Recycle Bin support when you are managing a subtree of a domain. If the domain access account does not have permissions on the hidden RecycleBin container in the specified domain, DRA cannot move deleted accounts to the Recycle Bin.

NOTE: After using this utility to enable the Recycle Bin, perform a full accounts cache refresh to ensure the Administration server applies this change.

You can use this utility to perform the following tasks:

- ♦ Verify that the specified account has read permissions on the RecycleBin container in the specified domain
- ♦ Delegate read permissions to a specified account
- ♦ Display security settings for the RecycleBin container

Required Permissions for the Recycle Bin Utility

To use this utility, you must have the following permissions:

If you want to ...	You need this permission ...
Verify account permissions	Read Permissions access to the RecycleBin container
Delegate read permissions on the RecycleBin container	Administrator permissions in the specified domain
Display security settings for the RecycleBin container	Read Permissions access to the RecycleBin container

Syntax for Recycle Bin Utility

```
DRARECYCLEBINUTIL /DOMAIN:DOMAINNAME [ /DC:COMPUTERNAME ] { /  
DELEGATE:ACCOUNTNAME | /VERIFY:ACCOUNTNAME | /DISPLAY }
```

Options for Recycle Bin Utility

The following options enable you to configure the Recycle Bin Utility:

- | | |
|------------------------------------|---|
| <i>/DOMAIN:domain</i> | Specifies the NETBIOS or DNS name of the domain where the Recycle Bin is located. |
| <i>/SERVER:computername</i> | Specifies the name or IP address of the domain controller for the specified domain. |

/DELEGATE: <i>accountname</i>	Delegates permissions to the specified account.
/VERIFY: <i>accountname</i>	Verifies permissions of the specified account.
/DISPLAY	Displays security settings for the RecycleBin container in the specified domain.

Examples for Recycle Bin Utility

The following examples demonstrate sample commands for common scenarios.

Example 1

To verify that the MYCOMPANY\JSmith user account has read permissions on the RecycleBin container in the hou.mycompany.com domain, enter:

```
DRARECYCLEBINUTIL /DOMAIN:HOU.MYCOMPANY.COM /VERIFY:MYCOMPANY\JSMITH
```

Example 2

To delegate read permissions on the RecycleBin container in the MYCOMPANY domain to the MYCOMPANY\DraAdmins group, enter:

```
DRARECYCLEBINUTIL /DOMAIN:MYCOMPANY /DELEGATE:MYCOMPANY\DRAADMINS
```

Example 3

To display security settings for the RecycleBin container in the hou.mycompany.com domain using the HQDC domain controller, enter:

```
DRARECYCLEBINUTIL /DOMAIN:HOU.MYCOMPANY.COM /DC:HQDC /DISPLAY
```

A Appendix

This appendix provides information about DRA Services and how to troubleshoot issues with the DRA REST Service.

- ◆ [“DRA Services” on page 229](#)
- ◆ [“Troubleshooting DRA REST Services” on page 230](#)
- ◆ [“Troubleshooting Installation and Upgrade” on page 233](#)

DRA Services

This table provides information on DRA services. This helps DRA administrators decide if they can safely disable a service without affecting any DRA functionality.

DRA Service	Description	Safe to disable
Administration Service	This service performs all the DRA operations and manages the internal DRA server processes.	No
DRA Audit Service	<p>This service handles the Unified Change History requests from the Web Console.</p> <p>When you disable this service:</p> <ul style="list-style-type: none">◆ DRA functionality is not impacted.◆ You will be able to generate Unified Change History reports from the Delegation and Configuration Console.◆ You will not be able to generate Unified Change History reports from the Web Console.	Yes
DRA Cache Service	This service acts as a persistent cache for the Administration Server.	No
DRA Core Service	<p>This service generates reports for DRA consoles and schedules the Active Directory, Office365, DRA, and Resource Collector jobs.</p> <p>When you disable this service:</p> <ul style="list-style-type: none">◆ DRA functionality is not impacted.◆ Collector jobs will not run so data for NRC reports will not be collected.◆ You will not be able to generate Unified Change History reports from any DRA console.	Yes
DRA Log Archive	This service stores all DRA audit events in a secure manner to support audit reporting.	No

DRA Service	Description	Safe to disable
DRA Replication Service	This service supports the DRA Temporary Group Assignment (TGA) feature. TGAs will not be available on any DRA server where this service is removed or stopped.	Yes
DRA Rest Service	The Web Console and PowerShell clients use this service to communicate with the Administration Server.	No
DRA Secure Storage	This service manages the AD LDS instance of DRA which stores the DRA configuration. It also replicates this configuration data across the MMS setup.	No
DRA Skype Service	This service manages all the Skype tasks. When you disable this service: <ul style="list-style-type: none"> ◆ DRA functionality is not impacted. ◆ Skype operations will not be processed. <p>NOTE: DRA Skype service will be deprecated from DRA version 10.3.</p>	Yes

Troubleshooting DRA REST Services

This section contains troubleshooting information for the following topics:

- ◆ [“Handling Certificates for the DRA REST Extensions” on page 230](#)
- ◆ [“Handling Errors from the DRA Server” on page 231](#)
- ◆ [“Every PowerShell Command Results in PSInvalidOperationException” on page 232](#)
- ◆ [“WCF Trace Logging” on page 232](#)

Handling Certificates for the DRA REST Extensions

The DRA endpoint service requires a certificate binding on the communication port. During installation, the installer will perform the commands for binding the port to the certificate. The purpose of this section is to describe how to validate the binding and how to add or remove a binding, if needed.

Basic Information

Default Endpoint Service Port: 8755

App ID for DRA REST Extensions: 8031ba52-3c9d-4193-800a-d620b3e98508

Certificate Hash: Displayed on the SSL Certificates page of the IIS Manager

Checking for Existing Bindings

In a CMD window, run this command: `netsh http show sslcert`

This will display a list of certificate bindings for this computer. Look through the list for the App ID of the DRA REST Extensions. The port number should match the config port. The certificate hash should match the certificate hash displayed in IIS Manager.

```
IP:port                : 0.0.0.0:8755
Certificate Hash       : d095304df3d3c8eecf64c25df7931414c9d8802c
Application ID        : {8031ba52-3c9d-4193-800a-d620b3e98508}
Certificate Store Name : (null)
Verify Client Certificate Revocation      : Enabled
Verify Revocation Using Cached Client Certificate Only : Disabled
Usage Check           : Enabled
Revocation Freshness Time : 0
URL Retrieval Timeout : 0
Ctl Identifier        : (null)
Ctl Store Name       : (null)
DS Mapper Usage      : Disabled
Negotiate Client Certificate : Disabled
```

Removing a Binding

To remove an existing binding, enter this command in a CMD window:

```
netsh http delete sslcert ipport=0.0.0.0:9999
```

Where 9999 is the port number to remove. The `netsh` command will display a message indicating that the SSL Certificate was successfully removed.

Adding a Binding

To add a new binding, enter the following command in a CMD window:

```
netsh http add sslcert ipport=0.0.0.0:9999 certhash=[HashValue]
appid={8031ba52-3c9d-4193-800a-d620b3e98508}
```

Where 9999 = the port number of the endpoint service and [HashValue] = the Certificate Hash value displayed in IIS Manager.

Handling Errors from the DRA Server

See the following if you get an error creating a mail-enabled object:

EnableEmail Returns Operation Failed

When creating a mail-enabled object or calling one of the EnableEmail endpoints, you might get an error back from the DRA server such as “*Server failed to complete the requested operation workflow successfully. Operation UserEnableEmail failed*”. This can be caused by including a mailNickname property in the payload that does not conform to the policy defined on the server.

Remove the mailNickname property from the payload and let the DRA server generate the email alias value according to the defined policy.

Every PowerShell Command Results in PSInvalidOperation Error

When you are the DRA REST service is bound to a self-signed certificate, the PowerShell cmdlets will return the following error:

```
Get-DRAServerInfo: One or more errors occurred.  
An error occurred while sending the request.  
The underlying connection was closed: Could not establish trust  
relationship for the SSL/TLS secure channel.  
The remote certificate is invalid according to the validation procedure.
```

On each command, you will need to include the `-IgnoreCertificateErrors` parameter. To also suppress the confirmation message, add the `-Force` parameter.

WCF Trace Logging

If your REST requests are resulting in errors that cannot be resolved by reading the REST service logs, you might need to raise the level of WCF’s trace logging to see details about how the request is traveling through the WCF layer. The volume of data generated by this level of the trace can be significant, so the shipped logging level is set to “Critical, Error”.

An example of when this might be useful is if the requests are resulting in null value exceptions even though you are sending the objects in the payload. Another case would be if the REST is becoming unresponsive.

To increase the WCF trace logging, you need to edit the configuration file for the service that is under scrutiny. Payload exceptions are likely to be evident from reviewing the WCF trace log for the REST Service.

Steps to Enable Detailed Logging

- 1 In Windows File Explorer, navigate to the DRA Extensions installation folder. Typically, this will be `C:\Program Files (x86)\NetIQ\DRA`.
- 2 Open the `NetIQ.DRA.RestService.exe.config` file.
- 3 Locate the `<source>` element in the following xml path:
`<system.diagnostics><sources>`
- 4 In the source element, change the `switchValue` attribute value from `"Critical, Error"` to `"Verbose, ActivityTracing"`.
- 5 Save the file and restart the DRA Rest Service.

EnableEmail Returns Operation Failed

The WCF trace data is written in a proprietary format. You can read the traces.svslog using the SvcTraceViewer.exe utility. You can find more information about this utility here: ([https://msdn.microsoft.com/en-us/library/ms732023\(v=vs.110\).aspx](https://msdn.microsoft.com/en-us/library/ms732023(v=vs.110).aspx))

Troubleshooting Installation and Upgrade

This section describes how to troubleshoot installation and upgrade issues.

Pre-requisites are missing error when you manage an Azure tenant

Troubleshooting Installation Issues with Microsoft.graph Version 2.9

1. Uninstall Microsoft.Graph version 2.9.
2. Install Microsoft.Graph version 2.8 by specifying the version number explicitly in the Install-Module cmdlet.

